AUTHORIZED DOCUMENTATION

Band I - Installationshandbuch

July, 2008

Novell® Sentinel®

6.1

www.novell.com

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für anstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 1999-2008 Novell, Inc., Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc. besitzt Anrechte auf geistiges Eigentum für Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite „Legal Patents“ von Novell (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Rechtliche Hinweise von Drittanbietern

In diesem Produkt sind möglicherweise die nachfolgend aufgeführten Open Source-Programme enthalten, die im Rahmen der Lesser General Public License-Lizenz (GNU) zur Verfügung gestellt werden. Den Lizenztext finden Sie im Verzeichnis „Licenses“.

edtFTPj-1.2.3 ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.enterprisedt.com/products/edtftpj/purchase.html (http://www.enterprisedt.com/products/edtftpj/purchase.html).

Enhydra Shark, lizenziert unter der Lesser General Public License, verfügbar unter: http://shark.objectweb.org/license.html (http://shark.objectweb.org/license.html).

Esper. Copyright © 2005-2006, Codehaus.

FESI ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.lugrin.ch/fesi/index.html (http://www.lugrin.ch/fesi/index.html).

jTDS-1.2.2.jar ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://jtds.sourceforge.net/ (http://jtds.sourceforge.net/).

MDateSelector. Copyright © 2005, Martin Newstead, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://web.ukonline.co.uk/mseries (http://web.ukonline.co.uk/mseries).

Tagish Java Authentication and Authorization Service Modules, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://free.tagish.net/jaas/index.jsp (http://free.tagish.net/jaas/index.jsp).

Dieses Produkt enthält möglicherweise Software, die von der Apache Software Foundation (http://www.apache.org/ (http://www.apache.org/)) entwickelt wurde und unter der Apache License, Version 2.0 („Lizenz“) lizenziert wurde. Den Lizenztext finden Sie im Verzeichnis „Licenses“ bzw. unter http://www.apache.org/licenses/LICENSE-2.0 (http://www.apache.org/licenses/LICENSE-2.0). Die unter dieser Lizenz vertriebene Software wird OHNE JEDWEDE MÄNGELGEWÄHR bereitgestellt, weder expliziter noch impliziter Art, solange dem nicht gültige Gesetzte entgegenstehen oder schriftlich Anderes vereinbart wurde. Informationen zu spezifischen sprachenrelevanten Rechten und Einschränkungen finden Sie in der Lizenz.

Apache Axis und Apache Tomcat, Copyright © 1999 bis 2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/. (http://www.apache.org/licenses/.)

Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Apache Lucene, Copyright © 1999 bis 2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Bean Scripting Framework (BSF), von der Apache Software Foundation lizenziert, Copyright © 1999-2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Lizenziert unter der Apache Software License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter https://skinlf.dev.java.net/ (https://skinlf.dev.java.net/).

Xalan und Xerces, jeweils von der Apache Software Foundation lizenziert, Copyright © 1999 - 2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

In diesem Produkt sind möglicherweise die nachfolgend aufgeführten Open Source-Programme enthalten, die im Rahmen der Java-Lizenz zur Verfügung gestellt werden.

JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javabeans/glasgow/jaf.html (http://www.java.sun.com/products/javabeans/glasgow/jaf.html), klicken Sie auf „Download“ > „License“.

Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html (http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html).

JavaMail. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javamail/downloads/index.html (http://www.java.sun.com/products/javamail/downloads/index.html), klicken Sie auf „Download“ > „License“.

In diesem Produkt sind möglicherweise die nachfolgend aufgeführten Open Source- und Drittanbieter-Programme enthalten.

ANTLR. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.antlr.org (http://www.antlr.org).

Boost. Copyright © 1999, Boost.org.

Concurrent, Dienstprogrammpaket. Copyright © Doug Lea. Wird ohne die Klassen CopyOnWriteArrayList und ConcurrentReaderHashMap verwendet.

ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003–2004.

ILOG, Inc. Copyright © 1999–2004.

Java Ace, von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University. Copyright © 1993-2005. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html (http://www.cs.wustl.edu/~schmidt/ACE-copying.html) und http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html (http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html).

Java Service Wrapper. Teile wie folgt durch Copyright geschützt: Copyright © 1999, 2004 Tanuki Software und Copyright © 2001 Silver Egg Technology. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://wrapper.tanukisoftware.org/doc/english/license.html (http://wrapper.tanukisoftware.org/doc/english/license.html).

JIDE. Copyright © 2002 bis 2005, JIDE Software, Inc.

JLDAP. Copyright © 1998-2005 The OpenLDAP Foundation. Alle Rechte vorbehalten. Copyright für Teile Copyright © 1999-2003 Novell, Inc. Alle Rechte vorbehalten.

Monarch Charts. Copyright © 2005, Singleton Labs.

OpenSSL, vom OpenSSL Project. Copyright © 1998 - 2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.openssl.org (http://www.openssl.org).

Oracle Help für Java. Copyright © 1994–2006, Oracle Corporation.

Rhino. Die Verwendung unterliegt der Mozilla Public License 1.1. Weitere Informationen finden Sie unter http://www.mozilla.org/rhino/ (http://www.mozilla.org/rhino/).

SecurityNexus. Copyright © 2003 bis 2006. SecurityNexus, LLC. Alle Rechte vorbehalten.

Sonic Software Corporation. Copyright © 2003 - 2004. Die SSC-Software enthält Sicherheitssoftware, die von RSA Security, Inc. lizenziert wurde.

Tao (mit ACE-Wrappers) von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University, University of California, Irvine und Vanderbilt University. Copyright © 1993-2005. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html (http://www.cs.wustl.edu/~schmidt/ACE-copying.html) und http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html (http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html).

Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://grinninglizard.com/tinyxmldocs/index.html (http://grinninglizard.com/tinyxmldocs/index.html).

XML Pull Parser. Dieses Produkt enthält Software, die von Indiana University Extreme! Lab (http://www.extreme.indiana.edu/ (http://www.extreme.indiana.edu/)) entwickelt wurde.

yWorks. Copyright © 2003 bis 2006, yWorks.

HINWEIS: Zum Zeitpunkt der Veröffentlichung dieser Dokumentation waren die oben stehenden Links aktiv. Sollten Sie feststellen, dass die oben stehenden Links unvollständig oder die verlinkten Webseiten inaktiv sind, wenden Sie sich an Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Inhalt

Vorwort **9**
Zielgruppe . . . 9
Rückmeldungen . . . 9
Zusätzliche Dokumentation . . . 9
Konventionen in der Dokumentation . . . 11
Anfragen an Novell . . . 11

1 Einführung **13**
1.1 Überblick über Sentinel . . . 13
1.2 Sentinel-Benutzeroberflächen . . . 14
1.2.1 Sentinel Control Center . . . 15
1.2.2 Sentinel Data Manager . . . 15
1.2.3 Sentinel Solution Designer . . . 15
1.2.4 Sentinel Collector Builder . . . 15
1.3 Sentinel-Serverkomponenten . . . 15
1.3.1 Sentinel-Server . . . 16
1.3.2 Sentinel Communication Server . . . 16
1.3.3 Sentinel-Datenbank . . . 16
1.3.4 Sentinel Collector Manager . . . 16
1.3.5 Correlation Engine . . . 16
1.3.6 iTRAC . . . 17
1.3.7 Crystal Reports Server . . . 17
1.3.8 Sentinel Advisor und Schwachstellenerkennung . . . 17
1.4 Sentinel-Plugins . . . 17
1.4.1 Collectors . . . 17
1.4.2 Connectors und Integratoren . . . 18
1.4.3 Korrelationsregeln und -aktionen . . . 18
1.4.4 Berichte . . . 18
1.4.5 iTRAC-Workflows . . . 18
1.4.6 Solution Packs . . . 19
1.5 Sprachunterstützung . . . 19

2 Systemanforderungen **21**
2.1 Unterstützte Software . . . 21
2.1.1 Unterstützte Datenbankplattformen . . . 22
2.1.2 Sentinel-Komponenten . . . 23
2.1.3 Plattformunterstützung: Ausnahmen und Warnhinweise . . . 25
2.2 Hardware-Empfehlungen . . . 26
2.2.1 Architektur . . . 26

3 Installieren von Sentinel 6.1 **31**
3.1 Übersicht über Installationsprogramm . . . 31
3.2 Sentinel-Konfigurationen . . . 32
3.2.1 Unter Solaris . . . 33
3.2.2 Unter Windows . . . 33
3.3 Allgemeine Voraussetzungen für die Installation . . . 34
3.3.1 Erteilen von Hauptbenutzer-Privilegien für „Domänenbenutzer“ . . . 35

3.3.2 Voraussetzungen für die Sentinel-Datenbankinstallation 35
3.3.3 Einstellungen des Authentifizierungsmodus unter Microsoft SQL 39
3.3.4 Voraussetzungen für die Sentinel-Serverinstallation 39
3.3.5 Voraussetzungen für die Advisor-Installation 39
3.4 Datenbankinstallation 39
3.4.1 Festlegen von Kernel-Werten 40
3.4.2 Erstellen von Gruppen- und Benutzerkonten für Oracle (nur bei Solaris) 42
3.4.3 Festlegen von Umgebungsvariablen für Oracle (nur bei Solaris) 42
3.4.4 Oracle installieren 43
3.5 Einfache Installation 43
3.6 Benutzerdefinierte Installation 46
3.6.1 Konsoleninstallation unter Linux/Solaris 57
3.7 Installation von Sentinel als Domänenbenutzer 59
3.8 Konfiguration nach der Installation 59
3.8.1 Konfigurieren des SMTP-Integrators für das Senden von S entinel-Benachrichtigungen 59
3.8.2 Sentinel-Datenbank 60
3.8.3 Collector-Service 60
3.8.4 Aktualisieren des Lizenzschlüssels (vom Evaluations- zum Produktionsschlüssel) . 61
3.8.5 Starten des Collector Manager Service 61
3.8.6 Zeitverwaltung 62
3.8.7 Bearbeiten der Oracle-Skripts „dbstart“ und „dbshut“ 62

4 Advisor-Konfiguration 65

4.1 Advisor-Überblick 65
4.2 Informationen zur Installation von Advisor 66
4.2.1 Einzelplatzkonfiguration 67
4.2.2 Konfiguration für direktes Herunterladen vom Internet 68
4.3 Installation von Advisor 68
4.3.1 Laden von Daten 71
4.3.2 Aktivieren von Advisor-Aktualisierungen 73
4.3.3 Verbindung mit dem Advisor-Server über einen Proxy 73
4.4 Advisor-Berichte 74
4.4.1 Konfiguration von Advisor-Berichten 74
4.5 Wartung von Advisor 75

5 Testen der Installation 77

5.1 Testen der Installation 77
5.2 Bereinigen nach Testen 84
5.3 Einführung 85

6 Hinzufügen von Sentinel-Komponenten 87

6.1 Hinzufügen von Sentinel-Komponenten zu einer bestehenden Installation 87
6.2 Installieren zusätzlicher Lastausgleichsknoten 87
6.2.1 Mehrere DAS_Binary-Prozesse 88

7 Kommunikationsschicht (iSCALE) 95

7.1 SSL-Proxy und direkte Kommunikation 96
7.1.1 Sentinel Control Center 96
7.1.2 Collector Manager 97
7.2 Ändern des Kommunikations-Verschlüsselungsschlüssels 99

7.3 Vergrößern der AES-Schlüsselstärke 100

8 Crystal Reports für Windows 101

8.1 Überblick 102
8.2 Systemanforderungen 103
8.3 Konfigurationsanforderungen 103
8.3.1 Installation von Microsoft Internet Information Server (IIS) und ASP.NET 104
8.4 Bekannte Probleme 105
8.5 Verwenden von Crystal Reports 105
8.6 Installationsüberblick 105
8.6.1 Installationsüberblick für Crystal mit SQL Server 2005 105
8.6.2 Installationsüberblick für Crystal mit Oracle 106
8.7 Installation 106
8.7.1 Installation von Crystal Reports Server für MS SQL Server 2005 mit Windows-Authentifizierung 106
8.7.2 Installation von Crystal Reports Server für Microsoft SQL Server 2005 mit SQL-Authentifizierung 112
8.7.3 Installation von Crystal Reports Server für Oracle 116
8.8 Konfiguration für alle Authentifizierungen und Konfigurationen 120
8.8.1 Konfiguration von inetmgr 120
8.9 Veröffentlichen Sie Crystal Reports-Schablonen 121
8.9.1 Veröffentlichen von Berichtsschablonen mit dem Lösungsmanager 121
8.9.2 Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard 121
8.9.3 Veröffentlichen von Reports-Schablonen – Central Management Console 123
8.9.4 Definieren eines benannten Benutzerkontos 124
8.9.5 Konfigurieren von Berichtsberechtigungen 125
8.9.6 Deaktivieren von Sentinel Top 10-Berichten 126
8.9.7 Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server 127
8.10 Auf Hochleistung ausgerichtete Konfigurationen für Crystal 128
8.10.1 Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung . . 128
8.10.2 Berichte, die den Aggregationsdienst verwenden. 129
8.10.3 Report Development 130

9 Crystal Reports für Linux 131

9.1 Überblick 132
9.2 Installation 132
9.2.1 Vorinstallation von Crystal Reports Server™ XI R2 132
9.2.2 Installation von Crystal Reports Server XI R2 134
9.3 Veröffentlichen von Crystal Reports-Schablonen 136
9.3.1 Veröffentlichen von Berichtsschablonen mit dem Lösungsmanager 136
9.3.2 Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard 136
9.3.3 Veröffentlichen von Reports-Schablonen – Central Management Console 138
9.4 Verwenden von Crystal XI R2 Web Server 139
9.4.1 Testen der Konnektivität zum Webserver 140
9.4.2 Festlegen eines Kontos für einen benannten Benutzer 140
9.4.3 Konfigurieren von Berichtsberechtigungen 140
9.5 Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung 141
9.6 Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server 142
9.7 Dienstprogramme und Fehlersuche 143
9.7.1 Starten von MySQL 143
9.7.2 Starten von Tomcat 143
9.7.3 Starten von Crystal Reports Server-Instanzen 143
9.7.4 Fehler beim Crystal-Hostnamen 143

9.7.5 Verbindung mit CMS nicht möglich 144
9.8 Auf Hochleistung ausgerichtete Konfigurationen für Crystal 145
9.8.1 Berichte, die den Aggregierungsdienst verwenden. 146
9.8.2 Report Development 146

10 Deinstallieren von Sentinel 147

10.1 Deinstallieren von Sentinel 147
10.1.1 Deinstallation unter Solaris und Linux 147
10.1.2 Deinstallation unter Windows 148
10.2 Nach der Deinstallation 149
10.2.1 Sentinel-Einstellungen 149

A Fragebogen vor der Installation 155

B Oracle-Setup 159

B.1 Installation von Oracle 159
B.1.1 Oracle 10g-Installation auf SLES 10 159
B.1.2 Oracle 10g Installation auf Red Hat Linux 4 160
B.1.3 Oracle 10g Installation auf Solaris 10 163
B.2 Manuelle Oracle-Instanzerstellung (optional) 163

C Sentinel mit Oracle Real Application Clusters 167

C.1 Konfigurieren der Oracle RAC-Datenbank 167
C.1.1 Erstellen der RAC-Datenbank 167
C.1.2 Erstellen von Sentinel-Tabellenbereichen 169
C.1.3 Erstellen von „ESECDBA“ 171
C.2 Erstellen der Sentinel-Datenbank 172
C.3 Konfigurieren der Datei mit den Verbindungseigenschaften 173
C.4 Konfigurieren der Verbindung für Sentinel Data Manager 174
C.5 Konfigurieren der Verbindung für Crystal 175

Vorwort

Sentinel™ ist eine Lösung für Sicherheitsinformationen und Ereignisverwaltung, die Informationen von zahlreichen Quellen im gesamten Unternehmen empfängt, standardisiert und priorisiert. Im Anschluss werden Ihnen diese Informationen präsentiert, um Sie bei Entscheidungen in Bezug auf Bedrohungen, Risiken und Richtlinien zu unterstützen.

Zielgruppe

Diese Dokumentation ist für Mitarbeiter des Bereichs Informationssicherheit konzipiert.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Onlinedokumentation, um Ihre Kommentare einzugeben.

Zusätzliche Dokumentation

Die technische Dokumentation von Sentinel umfasst sechs Bände. Dazu gehören:

- Sentinel 6.1-Installationshandbuch
- Sentinel 6.1-Benutzerhandbuch
- Sentinel 6.1-Referenzhandbuch für Benutzer
- Die Dokumentation zu diesem Produkt finden Sie unter http://www.novell.com/documentation/sentinel6/index.html

Band I – Sentinel-Installationshandbuch

In diesem Handbuch wird die Installation folgender Sentinel-Komponenten erläutert:

- Sentinel Communication Server
- Data Access Service-Prozess (DAS)
- Sentinel Control Center
- Sentinel Correlation Engine
- Collector Manager
- Crystal Reports Server
- Advisor
- Collector Builder
- Sentinel Data Manager
- Sentinel Solution Designer

Band II – Sentinel-Benutzerhandbuch

In diesem Handbuch wird die Verwendung der Komponenten und Funktionen von Sentinel erläutert:

- Verwendung der Sentinel Console
- Sentinel-Funktionen
- Sentinel-Architektur
- Sentinel Communication
- Herunterfahren/Starten von Sentinel
- Anfälligkeitsbewertung
- Ereignisüberwachung
- Ereignisfilterung
- Ereigniskorrelation
- Sentinel Data Manager
- Ereigniskonfiguration für Unternehmensrelevanz
- Zuordnungsservice
- Verlaufsberichte
- Collector-Host-Verwaltung
- Vorfälle
- Szenarios
- Benutzerverwaltung
- Workflow
- Solution Packs

Band III – Collector Builder-Benutzerhandbuch

In diesem Handbuch wird die Arbeit mit Collector Builder erläutert:

- Verwendung des Collector Builder
- Collector Manager
- Collectors
- Collector-Host-Verwaltung
- Erstellen und Warten von Collectors

Band IV – Sentinel-Referenzhandbuch für Benutzer

In diesem Handbuch werden folgende Themen für fortgeschrittene Benutzer erläutert:

- Collector-Skriptsprache
- Collector-Analysebefehle
- Collector-Administratorfunktionen
- Collector- und Sentinel-META-Tags
- Sentinel Correlation Engine
- Benutzerberechtigungen
- Korrelations-Befehlszeilenoptionen
- Sentinel-Datenbankschema

Band V – Sentinel-Handbuch zur Drittanbieterintegration

In diesem Handbuch wird die Verwendung von Sentinel mit verschiedenen Drittanbieteranwendungen erläutert.

- Remedy
- HP OpenView-Operationen
- HP Service Desk

Band VI – Sentinel-Handbuch zur Patchinstallation

In diesem Handbuch wird die Aufrüstung von einer Sentinel-Version auf die andere erläutert.

- Aufrüsten von Sentinel 4.x auf 6.0 mit Patches
- Aufrüsten von Sentinel 5.1.3 auf 6.0 mit Patches

Konventionen in der Dokumentation

In diesem Handbuch werden folgende Konventionen verwendet:

- Hinweise und Warnungen

  Hinweis: Bei Hinweisen handelt es sich um weitere Informationen, die hilfreich sein bzw. als Referenz herangezogen werden können.

  Warnung: Bei Warnungen handelt es sich um weitere Informationen, mit deren Hilfe Sie Systemaktionen identifizieren und unterlassen bzw. unterbinden können, die möglicherweise zu Beschädigung oder Datenverlust führen.

- Befehle sind in Courier-Schriftart angegeben. Beispiel:

  ```
  useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
  ```

- Wählen Sie zum Durchführen dieser Aktion die Optionsfolge „Start“ > „Programme“ > „Systemsteuerung“: Mehrere Aktionen in einer Anweisung
- Hinweise

  Weitere Informationen finden Sie unter “Abschnittsname” (wenn im selben Kapitel).

  Weitere Informationen finden Sie unter “Kapitelname” (wenn im selben Handbuch).

  Weitere Informationen finden Sie unter Abschnittsname in Kapitelname, *Name des Handbuchs* (wenn in einem anderen Handbuch).

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Nachrichten in einem Querverweispfad voneinander zu trennen.

Novellmarken werden durch das entsprechende Markensymbol (®, TM usw.) dargestellt, während Marken von Drittanbietern durch ein Sternchen (*) kenntlich gemacht werden.

Wenn ein Pfadname für bestimmte Plattformen mit einem umgekehrten Schrägstrich und für andere Plattformen mit einem Schrägstrich geschrieben werden kann, wird der Pfadname in diesem Handbuch mit einem umgekehrten Schrägstrich dargestellt. Benutzer von Plattformen wie Linux oder UNIX, die einen Schrägstrich erfordern, sollten wie von der Software gefordert Schrägstriche verwenden.

Anfragen an Novell

- Website: http://www.novell.com (http://www.novell.com)
- Novell Technical Support: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Self-Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site zum Herunterladen von Patches: http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)

- Support rund um die Uhr, sieben Tage pro Woche: http://www.novell.com/company/contact.html. (http://www.novell.com/company/contact.html.)
- Collectors/Connectors/Berichte/Korrelation/Hot Fixes/TIDS: http://support.novell.com/products/sentinel (http://support.novell.com/products/sentinel).

Einführung

1

- Abschnitt 1.1, „Überblick über Sentinel“, auf Seite 13
- Abschnitt 1.2, „Sentinel-Benutzeroberflächen“, auf Seite 14
- Abschnitt 1.3, „Sentinel-Serverkomponenten“, auf Seite 15
- Abschnitt 1.4, „Sentinel-Plugins“, auf Seite 17
- Abschnitt 1.5, „Sprachunterstützung“, auf Seite 19

In den nachfolgenden Abschnitten werden die Grundlagen des Produkts Schritt für Schritt erklärt. Der Rest des *Sentinel-Benutzerhandbuchs* besteht aus ausführlicheren Anweisungen hinsichtlich Architektur, Betrieb und Administration.

In diesen Abschnitten wird davon ausgegangen, dass Sie mit den Aspekten der Netzwerksicherheit, der Datenbankverwaltung sowie dem Windows*- und UNIX*-Betriebssystem vertraut sind.

1.1 Überblick über Sentinel

Sentinel™ ist eine Lösung für Sicherheitsinformationen und Ereignisverwaltung, die Informationen von zahlreichen Quellen im gesamten Unternehmen empfängt, standardisiert und priorisiert. Im Anschluss werden Ihnen diese Informationen präsentiert, um Sie bei Entscheidungen in Bezug auf Bedrohungen, Risiken und Richtlinien zu unterstützen.

Sentinel protokolliert Erfassungs-, Analyse- und Berichtsprozesse automatisch, um zu gewährleisten, dass die Bedrohungserkennung und die Audit-Anforderungen durch IT-Steuerelemente effektiv unterstützt werden. Mit Sentinel werden diese arbeitsaufwändigen manuellen Prozesse durch die automatisierte Dauerüberwachung von Sicherheits- und Konformitätsereignissen sowie IT-Steuerelementen ersetzt.

Sentinel sammelt in der gesamten Netzwerkinfrastruktur des Unternehmens sowie von Drittanbieter-Systemen, -Geräten und -Anwendungen sicherheitsbezogene und nicht sicherheitsbezogene Informationen und korreliert sie. Sentinel präsentiert die gesammelten Daten in einer übersichtlicheren und logischer aufgebauten grafischen Benutzeroberfläche (Graphical User Interface, GUI), identifiziert Sicherheits- bzw. Konformitätsprobleme und verfolgt die Behebungsmaßnahmen – auf diese Weise werden ehemals fehleranfällige Prozesse optimiert und es entsteht ein strikteres und sichereres Verwaltungsprogramm.

Mithilfe der automatisierten Vorfallsreaktions-Verwaltung können Sie den Prozess der Verfolgung, Eskalation und Reaktion auf Vorfälle und Richtlinienverstöße dokumentieren und formalisieren. Außerdem wird die bidirektionale Integration in Problemberichtssysteme ermöglicht. Mit Sentinel können Sie prompt reagieren und Vorfälle auf effiziente Weise aus der Welt schaffen.

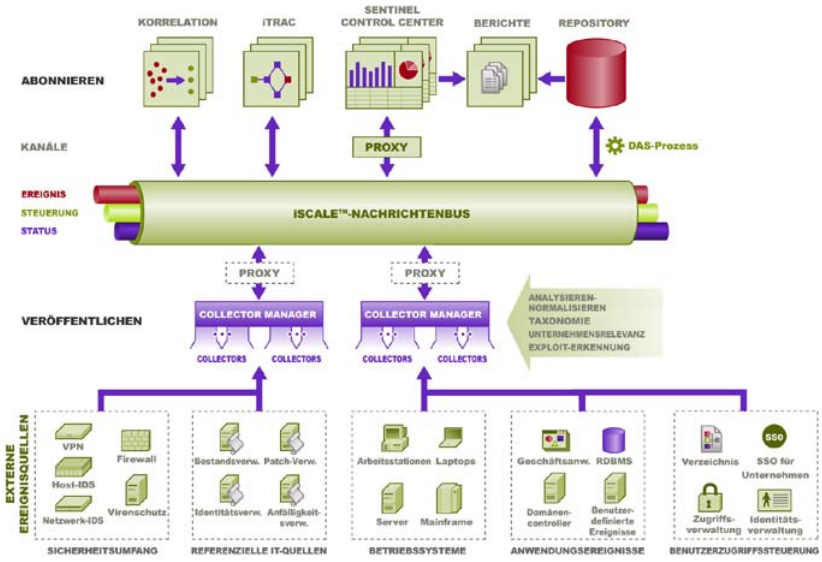
Mithilfe von Solution Packs können Sentinel-Korrelationsregeln, dynamische Listen, Zuordnungen, Berichte sowie iTRAC-Workflows mühelos verteilt und in Steuerelemente importiert werden. Diese Steuerelemente können für die Einhaltung spezifischer behördlicher Bestimmungen, beispielsweise dem Payment Card Industry Data Security Standard, konfiguriert oder mit einer spezifischen Datenquelle, beispielsweise Benutzerauthentifizierungsereignissen für eine Oracle-Datenbank, verknüpft werden.

Sentinel bietet die folgenden Vorteile:

- Integrierte, automatisierte Sicherheitsverwaltung und Konformitätsüberwachung in sämtlichen Systemen und Netzwerken – in Echtzeit
- Ein Framework, innerhalb dessen IT-Richtlinien und -Vorgehensweisen maßgeblich von den Geschäfsanforderungen gesteuert werden
- Automatische Dokumentation und Berichterstellung in Bezug auf Sicherheits-, System- und Zugriffsereignisse im gesamten Unternehmen
- Integrierte Vorfallsverwaltung und -beseitigung
- Umsetzung und Überwachung der Konformität mit internen Richtlinien und Bestimmungen von Regierungsbehörden, wie etwa dem Sarbanes-Oxley Act, dem Health Insurance Portability and Accountability Act (HIPAA), dem Gramm Leach Bliley Act (GLBA) und dem Federal Information Security Management Act (FISMA), um nur einige zu nennen. Die für die Implementierung dieser Steuerelemente erforderlichen Inhalte werden ganz einfach mithilfe von Solution Packs verteilt und implementiert.

Hier sehen Sie die konzeptuelle Architektur von Sentinel, die Aufschluss über die an der Sicherheits- und Konformitätsverwaltung beteiligen Komponenten gibt.

Abbildung 1-1 *Konzeptuelle Architektur von Sentinel*



1.2 Sentinel-Benutzeroberflächen

In Sentinel gibt es mehrere benutzerfreundliche Benutzeroberflächen:

- Sentinel Control Center
- Sentinel Data Manager
- Sentinel Solution Designer
- Sentinel Collector Builder

1.2.1 Sentinel Control Center

Das Sentinel Control Center bietet eine integrierte Sicherheitsverwaltungskonsole, mit der Sicherheitsanalytiker schnell neue Trends oder Angriffe erkennen, grafische Informationen in Echtzeit bearbeiten und damit interagieren sowie auf Vorfälle reagieren können. Sentinel Control Center beinhaltet folgende wichtige Funktionen:

- **Active Views:** Analysefunktionen und Visualisierung in Echtzeit
- **Vorfälle:** Erstellung und Verwaltung von Vorfällen
- **Korrelation:** Definition und Verwaltung von Korrelationsregeln
- **iTRAC:** Prozessverwaltung für Dokumentation, Erzwingung und Verfolgung von Prozessen zur Vorfallsauflösung
- **Berichterstellung:** Verlaufsberichte und Metriken
- **Ereignisquellenverwaltung** Collector-Bereitstellung und -Überwachung

1.2.2 Sentinel Data Manager

Mit Sentinel Data Manager (SDM) können Sie die Sentinel-Datenbank verwalten. In SDM können Sie folgende Vorgänge durchführen:

- Nutzung des Datenbankspeichers überwachen
- Datenbankpartitionen anzeigen und verwalten
- Datenbankarchive verwalten
- Daten in die Datenbank importieren

1.2.3 Sentinel Solution Designer

Sentinel Solution Designer dient der Erstellung und Modifizierung von Solution Packs. Hierbei handelt es sich um Pakete mit Sentinel-Inhalten, beispielsweise Berichte, Korrelationsregeln und Workflows.

1.2.4 Sentinel Collector Builder

Mit Sentinel Collector Builder können Sie Collectors zur Prozessverarbeitung in der Sentinel-eigenen Sprache erstellen. Sie können Schablonen erstellen und so anpassen, dass der jeweilige Collector die Daten analysieren kann.

1.3 Sentinel-Serverkomponenten

Sentinel besteht aus mehreren Komponenten:

- Data Access Service-Prozess (DAS)
- Sentinel Communication Server
- Sentinel-Datenbank
- Sentinel Collector Manager
- Correlation Engine

- iTRAC™
- Crystal Reports Server *
- Sentinel Advisor und Schwachstellenerkennung (optional)

1.3.1 Sentinel-Server

Data Access Service (DAS) ist die Primärkomponente, die zur Kommunikation mit der Sentinel-Datenbank verwendet wird. DAS sorgt gemeinsam mit anderen Server-Komponenten dafür, dass von den Collector Managers übermittelte Ereignisse in der Datenbank gespeichert, Daten gefiltert, Active View-Anzeigen verarbeitet, Datenbankabfragen durchgeführt, Ergebnisse verarbeitet sowie administrative Aufgaben, beispielsweise Benutzerauthentifizierung und -autorisierung, verwaltet werden.

1.3.2 Sentinel Communication Server

Der Nachrichten-Bus iSCALE™ kann in einer einzigen Sekunde Tausende Nachrichtenpakete zwischen den Komponenten von Sentinel verschieben. Auf diese Weise werden die Skalierung von Komponenten sowie die auf Standards basierende Integration in externe Anwendungen ermöglicht.

1.3.3 Sentinel-Datenbank

Kernstück des Sentinel-Produkts ist eine Backend-Datenbank zur Speicherung von Sicherheitsereignissen und sämtlichen Sentinel-Metadaten. Die Ereignisse werden in normalisierter Form gespeichert, ebenso wie Bestands- und Anfälligkeitsdaten, Identitätsinformationen, Vorfalls- und Workflow-Status, und zahlreiche andere Arten von Daten.

1.3.4 Sentinel Collector Manager

Der Collector Manager verwaltet die Datenerfassung, überwacht Meldungen zum Systemstatus und führt die Ereignisfilterung durch – ganz nach Bedarf. Zu den Hauptfunktionen des Collector Managers zählen das Umwandeln von Ereignissen, das Hinzufügen von Geschäftsrelevanz zu Ereignissen über die Taxonomie, das Durchführen globaler Filtervorgänge für Ereignisse, das Routing von Ereignissen sowie das Senden von Zustandsmeldungen an den Sentinel-Server.

Der Sentinel Collector Manager kann eine direkte Verbindung zum Nachrichten-Bus herstellen oder einen Secure Sockets Layer-(SSL-)Proxy nutzen.

1.3.5 Correlation Engine

Durch die Korrelationsanalyse wird die Verwaltung von Sicherheitsereignissen aussagekräftiger, da auffällige Ereignismuster im eingehenden Datenstrom leichter identifiziert werden können. Die Korrelation ermöglicht Ihnen das Definieren von Regeln, die kritische Bedrohungen und komplexe Angriffsmuster identifizieren, sodass Sie Ereignissen Priorität verleihen und eine effektive Vorfallsverwaltung und -reaktion initialisieren können.

1.3.6 iTRAC

Sentinel stellt ein iTRAC-Workflow-Verwaltungssystem bereit, mit dem Prozesse für die Vorfallsreaktion definiert und automatisiert werden können. Vorfälle, die in Sentinel identifiziert werden (entweder durch eine Korrelationsregel oder manuell), können mit einem iTRAC-Workflow verknüpft werden.

1.3.7 Crystal Reports Server

Hinter den umfassenden Berichtservices im Sentinel Control Center steht Crystal Reports Server von Business Objects*. Sentinel enthält vordefinierte Berichte, die sich an den gängigsten Anforderungen von Unternehmen hinsichtlich Sicherheits- und Konformitätsüberwachungen orientieren. Mit Crystal Reports Developer können neue oder individuell angepasste Berichte zudem anhand des von Sentinel ausgegebenen Berichtansichtsschemas erstellt werden.

1.3.8 Sentinel Advisor und Schwachstellenerkennung

Sentinel Advisor ist ein optionaler Datenabonnement-Service mit Informationen zu bekannten Angriffen, Anfälligkeiten und Gegenmaßnahmen. Diese Daten ermöglichen, in Kombination mit Informationen zu bekannten Anfälligkeiten sowie Echzeit-Informationen zu Intrusion Detection (Eindringversuchserkennung) und der entsprechenden Gegenmaßnahmen aus Ihrer Systemumgebung, die proaktive Schwachstellenerkennung. Zudem kann im Falle eines Angriffs eines anfälligen Systems sofort reagiert werden.

1.4 Sentinel-Plugins

Sentinel unterstützt eine Reihe von Plugins zur Erweiterung und Optimierung der Systemfunktionalität. Einige dieser Plugins werden automatisch installiert. Weitere Plugins (und Updates) können unter http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html) heruntergeladen werden.

Für einige Plugins, etwa Remedy* Integrator und IBM* Mainframe Connector, ist zum Herunterladen eine zusätzliche Lizenz erforderlich.

1.4.1 Collectors

Sentinel sammelt Daten von Quellgeräten und stellt einen umfassenderen Ereignisdatenstrom bereit, indem Taxonomie, Schwachstellenerkennung sowie Geschäftsrelevanz in den Datenstrom integriert werden, bevor Ereignisse korreliert, analysiert und an die Datenbank gesendet werden. Ein umfangreicherer Ereignisstrom bedeutet, dass die Daten mit dem erforderlichen Geschäftskontext korreliert werden, um interne bzw. externe Bedrohungen und Richtlinienverletzungen erkennen und beheben zu können.

Sentinel-Collectors können Daten von folgenden Komponenten analysieren:

◆ Intrusion Detection-Systeme (Host)	◆ Virenschutzsysteme
◆ Intrusion Detection-Systeme (Netzwerk)	◆ Webserver
◆ Firewalls	◆ Datenbanken
◆ Betriebssysteme	◆ Mainframe
◆ Richtlinienüberwachung	◆ System zur Anfälligkeitsbewertung
◆ Authentifizierung	◆ Directory Services
◆ Router und Switches	◆ Netzwerkverwaltungssysteme
◆ VPNs	◆ Proprietäre Systeme

JavaScript-Collectors können mit Sentinel 6.0 SP1 und höher erstellt und ausgeführt werden, unter Verwendung standardmäßiger JavaScript-Entwicklungstools und des Software Development Kit (SDK) für Collectors. Proprietäre Collectors können mithilfe von Abschnitt 1.2.4, „Sentinel Collector Builder“, auf Seite 15 erstellt oder modifiziert werden, einer eigenständigen Anwendung, die Teil des Sentinel-Systems ist.

1.4.2 Connectors und Integratoren

Connectors stellen über Standardprotokolle wie JDBC (Java Database Connectivity) und syslog die Verbindung zwischen dem Collector Manager und Ereignisquellen her. Ereignisse werden zu Analysezwecken vom Connector an den Collector übertragen.

Integratoren ermöglichen die Durchführung von Gegenmaßnahmen auf Systemen außerhalb von Sentinel. So kann beispielsweise eine Korrelationsaktion den Simple Object Access Protocol-(SOAP-)Integrator zur Initiierung eines Novell Identity Manager-Workflows nutzen.

Mit dem optionalen Remedy AR-Integrator kann ein Remedy-Bericht anhand von Sentinel-Ereignissen oder -Vorfällen erstellt werden.

1.4.3 Korrelationsregeln und -aktionen

Anhand von Korrelationsregeln werden wichtige Muster im Ereignis-Stream identifiziert. Wenn eine Korrelationsregel ausgelöst wird, initiiert sie Korrelationsaktionen. So werden beispielsweise Email-Benachrichtigungen gesendet, ein iTRAC-Workflow wird initiiert oder es wird mithilfe eines Integrators eine Aktion ausgeführt.

1.4.4 Berichte

Im Sentinel Control Center können die Benutzer mit Crystal Reports Server viele unterschiedliche Dashboard- und Betriebs-Berichte ausführen. Ab Sentinel 6.1 werden Berichte in der Regel über Solution Packs verteilt.

1.4.5 iTRAC-Workflows

iTRAC-Workflows sorgen für konsistente, wiederholbare Prozesse beim Verwalten von Vorfällen. Ab Sentinel 6.1 werden Workflow-Schablonen in der Regel über Solution Packs verteilt.

1.4.6 Solution Packs

Solution Packs sind Pakete mit verwandten Sentinel-Inhalten, etwa Korrelationsregeln, Aktionen, iTRAC-Workflows und Berichten. Novell stellt Solution Packs bereit, die auf spezifische Anforderungen im Geschäftsleben ausgerichtet sind. So liegt beim PCI-DSS Solution Pack der Schwerpunkt beispielsweise auf der Konformität mit dem Payment Card Industry Data Security Standard. Novell erstellt zudem „Collector Packs“, bei denen der Schwerpunkt der jeweiligen Inhalte auf einer spezifischen Ereignisquelle liegt, beispielsweise Windows Active Directory.

1.5 Sprachunterstützung

Sentinel-Komponenten werden für folgende Sprachen lokalisiert:

- Englisch
- Portugiesisch (Brasilien)
- Französisch
- Italienisch
- Deutsch
- Spanisch
- Japanisch
- Chinesisch (Traditionell)
- Chinesisch (Vereinfacht)

Es gibt einige Ausnahmen:

- Collector Builder-Schnittstelle und -Skripterstellung sind nur auf Englisch verfügbar, das Programm kann jedoch unter den oben aufgeführten nichtenglischen Betriebssystemen ausgeführt werden.
- JavaScript-Collectors können so angepasst werden, dass entweder Daten im Format American Standard Code for Information Interchange (ASCII) oder Unicode (Doppelbyte) analysiert werden. Die auf der Sentinel Content-Website veröffentlichten Collectors sind zurzeit jedoch lediglich für englische Daten geschrieben. In der proprietären Collector-Sprache geschriebene Collectors können nur Daten im ASCII- und Extended ASCII-Format verarbeiten.
- Interne Ereignisse (zur Prüfung von Sentinel-Vorgängen) sind ausschließlich auf Englisch.

Systemanforderungen

2

- Abschnitt 2.1, „Unterstützte Software“, auf Seite 21
- Abschnitt 2.2, „Hardware-Empfehlungen“, auf Seite 26

2.1 Unterstützte Software

Für optimale Leistung und Zuverlässigkeit empfiehlt Novell dringend, sämtliche Sentinel-Komponenten nur mit anerkannter Software zu verwenden, die umfassend geprüft und 100%ig zertifiziert wurde. Die jeweils aktuellen Informationen zu den Mindestanforderungen finden Sie in den Updates auf der Website zur Novell-Dokumentation (http://www.novell.com/documentation/sentinel61).

In der nachfolgenden Tabelle sind die spezifischen Patch-Level angegeben, die beim Testen von Sentinel zum Einsatz kamen. Aus Gründen der Übersichtlichkeit wird in diesem Dokument für diese Plattformen der Kurzname in der linken Spalte verwendet. In Fällen, in denen die Bit-Länge in diesem Dokument keine Rolle spielt, wird die Bit-Länge möglicherweise vom Kurznamen abgeschnitten.

Tabelle 2-1 *Informationen zum Patch-Level*

Kurzname	Vollständiger Name und Patch-Level
SLES 10 (32 Bit)	SUSE® Linux Enterprise Server 10 SP1 (32 Bit)
SLES 10 (64 Bit)	SUSE Linux Enterprise Server 10 SP1 (64 Bit)
RHEL 4 (32 Bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (32 Bit)
RHEL 4 (64 Bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (64 Bit)
Solaris 10 (64-Bit)	Sun Solaris 10 6/06 s10s_u2wos_09a (SPARC (64 Bit))
Windows 2003 (32 Bit)	Windows 2003 SP2, Standard oder Enterprise Edition (32 Bit)
Windows 2003 (64 Bit)	Windows 2003 SP1, Standard oder Enterprise Edition (64 Bit)
Windows 2008 (64 Bit)	Windows 2008 SP1, Standard Edition (64 Bit)
SLED 10 (32 Bit)	SUSE® Linux Enterprise Desktop 10 SP1 (32 Bit)
Windows XP (32 Bit)	Windows XP SP2 (32 Bit)
Windows Vista (32 Bit)	Windows Vista SP1 (32 Bit)
Oracle 10 (32 Bit)	Oracle* 10g Enterprise Edition mit Partitionierung (V 10.2.0.3 – 5901891 mit kritischem Patch Nr. 5881721, Sicherheits-Patch 6864068) (32 Bit), unter SuSE Linux Enterprise Server 10 (32 Bit)
Oracle 10 (64 Bit)	Oracle 10g Enterprise Edition mit Partitionierung (V 10.2.0.3 – 5901891 mit kritischem Patch Nr. 5881721, Sicherheits-Patch 6864068), unter SuSE Linux Enterprise Server 10 (64 Bit)
SQL Server 2005 (32 Bit)	Microsoft SQL Server 2005 SP2, Standard oder Enterprise Edition (32 Bit)

Kurzname	Vollständiger Name und Patch-Level
SQL Server 2005 (64 Bit)	Microsoft SQL Server 2005 SP2, Standard oder Enterprise Edition (64 Bit)
SQL Server 2008 (64 Bit)	Microsoft SQL Server 2008 CTP Februar 2008 (64 Bit)
SLES 9 (32 Bit)	SuSE Linux Enterprise Server 9 SP2 (32 Bit)

Überprüfen Sie die Websites der jeweiligen Hersteller auf Sicherheitsupdates und -patches. Diese Hotfixes und Sicherheitspatches haben normalerweise keinen Einfluss auf die Funktionsweise von Sentinel und werden daher unterstützt. Da bei der Freigabe von Haupt- oder Nebenversionen einer Datenbank oder eines Betriebssystems häufig mehrere wesentliche Änderungen vorgenommen wurden, werden für dieses Release nur die oben angegebenen Versionen unterstützt.

2.1.1 Unterstützte Datenbankplattformen

Die nachfolgend aufgeführten Datenbank-Betriebssystem-Kombinationen sind als zertifiziert oder unterstützt gekennzeichnet. Zertifizierte Kombinationen wurden mithilfe der vollständigen Testsuite von Novell Engineering getestet. Unterstützte Kombinationen verfügen über vollen Funktionsumfang.

Tabelle 2-2 *Unterstützte Datenbankplattformen*

	Oracle 10 (32)	Oracle 10 (64)	SQL Server 2005 (32)	SQL Server 2005 (64)	MS SQL 2008 (64)
SLES 10 (32)	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
SLES 10 (64)	Nicht unterstützt	Zertifiziert	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
RHEL 4 (32)	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
RHEL 4 (64)	Nicht unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Solaris 10 (32)	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Solaris 10 (64)	Nicht unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 2003 (32)	Nicht unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 2003 (64)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Zertifiziert	Nicht unterstützt
Windows 2008 (64)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt

Auch wenn in Entwicklungs- oder Testumgebungen 32-Bit-Plattformen für die Sentinel-Datenbank unterstützt werden, empfiehlt Novell 64-Bit-Plattformen für Produktionsdatenbanken, um optimale Leistungen zu erzielen.

Sentinel wurde mit der Beta-Version von Microsoft SQL Server 2008 CTP Februar 2008 (64 Bit) getestet. Zum Zeitpunkt der Veröffentlichung lagen keine bekannten Probleme vor. Etwaige Änderungen an der Datenbank, die vor der offiziellen Veröffentlichung erfolgen, können sich jedoch auf die Funktionsweise von Sentinel auswirken.

Hinweis: Sämtliche Datenbanken sollten unter einem Betriebssystem installiert werden, das sowohl vom Datenbankhersteller als auch von Novell zur Verwendung mit Sentinel-Komponenten zertifiziert wurde. Oracle muss unter Linux* oder Solaris (nicht unter Windows) ausgeführt werden.

2.1.2 Sentinel-Komponenten

Zu den Sentinel-Serverkomponenten zählen Communication Server, Correlation Engine, Data Access Service (DAS) sowie der Advisor-Datenabonnementservice (auf demselben Computer wie DAS).

Zu den Sentinel-Benutzeranwendungen in der nachfolgenden Tabelle zählen Sentinel Control Center, Sentinel Data Manager und Sentinel Solution Designer.

Für Collector Manager, Collector Builder und Crystal Reports Server liegen ebenfalls bestimmte Plattformanforderungen vor.

Die nachfolgend aufgeführten Software-Betriebssystem-Kombinationen sind als zertifiziert (C) oder unterstützt (S) gekennzeichnet. Zertifizierte Kombinationen wurden mithilfe der vollständigen Testsuite von Novell Engineering getestet. Unterstützte Kombinationen verfügen über vollen Funktionsumfang.

Tabelle 2-3 *Software- und Betriebssystem-Kombinationen*

	Sentinel-Serverkomponenten	Sentinel-Benutzeranwendungen	Collector Manager	Collector Builder	Crystal Reports Server
SLES 10 (32)	Unterstützt	Unterstützt	Zertifiziert	Nicht unterstützt	Nicht unterstützt
SLES 10 (64)	Zertifiziert	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
RHEL 4 (32)	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt	Zertifiziert
RHEL 4 (64)	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Solaris 10 (32)	Unterstützt	Unterstützt	Zertifiziert	Nicht unterstützt	Nicht unterstützt
Solaris 10 (64)	Zertifiziert	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt

	Sentinel-Serverkomponenten	Sentinel-Benutzeranwendungen	Collector Manager	Collector Builder	Crystal Reports Server
Windows 2003 (32)	Unterstützt	Unterstützt	Zertifiziert	Unterstützt	Zertifiziert
Windows 2003 (64)	Zertifiziert	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
Windows 2008 (64)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
SLED 10	Nicht unterstützt	Zertifiziert	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows XP	Nicht unterstützt	Zertifiziert	Nicht unterstützt	Unterstützt	Nicht unterstützt
Windows Vista	Nicht unterstützt	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
SLES 9 (32)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Zertifiziert

Crystal Reports Server XI R2 ist der unterstützte Berichtsserver. Für Crystal sind neben der Sentinel-Datenbank ein Webserver und eine Central Management Server-(CMS-)Datenbank erforderlich. Die Crystal Reports Server-Ausführung ist in der Sentinel-Umgebung auf folgenden Plattformen möglich:

- Red Hat Enterprise Linux 4 (32 Bit)
  - Crystal CMS-Datenbank mit MySQL
  - Webserver auf Apache Tomcat
  - Sentinel-Datenbank unter Oracle empfohlen, andere Konfigurationen wurden nicht getestet.
- SuSE Linux Enterprise Server 9 SP2 (32 Bit)
  - Crystal CMS-Datenbank mit MySQL
  - Webserver auf Apache Tomcat
  - Sentinel-Datenbank unter Oracle empfohlen, andere Konfigurationen wurden nicht getestet.
- Windows 2003 SP1 Server, Standard oder Enterprise Edition (32 Bit)
  - Crystal CMS-Datenbank mit Microsoft SQL Server 2005
  - Webserver mit Microsoft IIS mit .NET
  - Sentinel-Datenbank unter SQL Server empfohlen, andere Konfigurationen wurden nicht getestet.

Novell hat mit folgenden Crystal-Versionen das Veröffentlichen und Ausführen von Berichten über die Sentinel-Schnittstelle getestet:

- **Unter Linux:** Crystal Reports Server XI R2 SP2
- **Unter Windows:** Crystal Reports Server XI R2 SP3

Diese Service Packs können im Download-Bereich der SAP-Website heruntergeladen werden:

https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads)

Ziehen Sie hinsichtlich weiterer Informationen zu Systemanforderungen, unterstützten Versionsnummer und bekannten Problemen in Bezug auf diese Plattformen die Herstellerdokumentation zurate.

2.1.3 Plattformunterstützung: Ausnahmen und Warnhinweise

Folgende Plattformen werden vom jeweiligen Hersteller und folglich auch von Novell nicht unterstützt:

- Der Hersteller von Crystal Reports Server XI R2 unterstützt Crystal unter Solaris oder unter SUSE Linux Enterprise Server 10 zurzeit nicht. Aus diesem Grund unterstützt Novell diese Kombinationen ebenfalls nicht.
- Oracle unterstützt zurzeit Oracle 10 (32 Bit) unter Solaris 10 (32 Bit) nicht.

Obwohl folgende Plattformkonfigurationen möglicherweise vom jeweiligen Hersteller unterstützt werden, rät Novell von diesen Konfigurationen in einer Sentinel-Umgebung ab:

- Sentinel unter SUSE Linux Enterprise Server 10 mit ReiserFS-Dateisystem
- Oracle-Datenbank unter Microsoft Windows
- Crystal Reports Server unter Microsoft Windows 2000
- Crystal Reports Server mit MSDE als Datenbank

Novell empfiehlt, die Sentinel-Datenbank- und Berichts-Engine auf Plattformen auszuführen, die von Novell umfassend getestet wurden, jedoch werden sowohl die Oracle-Datenbank als auch Crystal Reports Server auf zusätzlichen Plattformen vom jeweiligen Hersteller unterstützt. Wenn ein Kunde eine dieser zusätzlichen Plattformen nutzen möchte, bietet Novell unter Vorbehalt eingeschränkten Support an.

- Da Installation und Konfiguration der Sentinel-Datenbank plattformabhängig sind, sollte Novell Consulting oder ein qualifizierter Partner mit der erstmaligen Installation und Einrichtung von Sentinel beauftragt werden.
- Das Standardinstallationsprogramm funktioniert auf einer nicht getesteten Plattform möglicherweise nicht erwartungsgemäß.
- Nachdem die Funktionsfähigkeit des Sentinel-Systems gewährleistet wurde, liegt jegliches Datenbank- bzw. Berichtsproblem, das auf den von uns unterstützten In-House-Plattformen nicht dupliziert werden kann, in der Verantwortung des jeweiligen Herstellers.

Zudem empfiehlt Novell – zur Gewährleistung der uneingeschränkten Funktionalität – die Installation von Datenbank und DAS unter ein- und demselben Betriebssystem (jedoch nicht unbedingt auf demselben Computer). (Beispiel: Die Windows-Authentifizierung kann nicht verwendet werden, wenn die Installation in einer gemischten Umgebung erfolgt (DAS unter Windows und Oracle-Datenbank bzw. DAS unter UNIX oder Linux und SQL Server-Datenbank.))

Collector Builder kann nur auf Windows-Plattformen ausgeführt werden.

2.2 Hardware-Empfehlungen

Bei der Installation unter Linux oder Windows kann für die Sentinel-Server- und Datenbankkomponenten Hardware vom Typ x86 (32 Bit) oder x86-64 (64 Bit) verwendet werden. Es gibt einige auf das Betriebssystem bezogene Ausnahmen, wie oben erläutert. Sentinel ist für AMD Optero- und Intel Xeon-Hardware zertifiziert. Itanium-Server werden nicht unterstützt.

Für Solaris wird die SPARC-Architektur unterstützt.

Warnung: Da Sentinel ein Hochleistungsprodukt ist, empfiehlt Novell, Sentinel in Produktionsumgebungen auf dedizierter Hardware auszuführen, nicht auf virtuellen Maschinen (auch: VMs).

2.2.1 Architektur

Sentinel weist eine hochgradig skalierbare Architektur auf. Wenn ein großes Ereignisaufkommen erwartet wird, können Komponenten auf mehrere Computer verteilt und so die optimale Leistung des Systems erzielt werden.

Beim Entwurf eines Sentinel-Systems sollten zahlreiche Faktoren berücksichtigt werden. Hier eine Teilliste mit Faktoren, die beim Ausarbeiten eines Entwurfs berücksichtigt werden müssen.

- Ereignisrate (Events Per Second, EPS)
- Geografischer Standort/Netzwerkstandort von Ereignisquellen sowie Bandbreite beim Austausch zwischen Netzwerken
- Verfügbare Hardware
- Bevorzugte Betriebssysteme
- Pläne hinsichtlich künftiger Skalierbarkeit
- Erwarteter Ereignisfilterungsumfang
- Örtliche Vorschriften zur Datenaufbewahrungspflicht
- Gewünschte Anzahl und Komplexität von Korrelationsregeln
- Erwartete Vorfallszahl pro Tag
- Erwartete Anzahl von Workflows, die pro Tag verarbeitet werden.
- Anzahl der Benutzer, die sich beim System anmelden.
- Anfälligkeit und Bestandsinfrastruktur

Der wichtigste Faktor beim Entwurf des Sentinel-Systems ist die Ereignisrate; nahezu jede Komponente der Sentinel-Architektur ist von steigenden Ereignisraten betroffen. Bei einer hohen Ereignisrate liegt die größte Belastung auf der Datenbank, die ausgesprochen E/A-abhängig ist und u. U. pro Sekunde Tausende Einfügevorgänge von Hunderten oder Tausenden Ereignissen, die Objekterstellung durch mehrere Benutzer, Workflow-Prozessaktualisierungen, einfache Verlaufsabfragen vom Sentinel Control Center sowie langfristige Berichte von Crystal Reports Server verarbeitet. Aus diesem Grund spricht Novell folgende Empfehlungen aus:

- Die Datenbank sollte ohne weitere Sentinel-Komponenten installiert werden.
- Der Datenbankserver sollte für Sentinel-Vorgänge dediziert sein. Zusätzliche Anwendungen oder Extract Transform Load-(ETL-)Vorgänge (zum Extrahieren, Transformieren und Laden) können die Leistung der Datenbank beeinträchtigen.

- Der Datenbankserver sollte über ein Hochgeschwindigkeits-Speicher-Array verfügen, das der E/A-Anforderung basierend auf den Ereigniseinfügeraten gerecht wird.
- Ein verantwortlicher Datenbankadministrator sollte folgende Datenbankinformationen regelmäßig auswerten und pflegen:
  - Größe
  - E/A-Vorgänge
  - Festplattenspeicher
  - Arbeitsspeicher
  - Indizierung
  - Transaktionsprotokolle

Bei niedriger Ereignisrate (Beispiel: EPS < 25) können die obigen Empfehlungen weniger strikt interpretiert werden, da die Datenbank und andere Komponenten weniger Ressourcen beanspruchen.

In diesem Abschnitt finden Sie einige allgemeine Hardware-Empfehlungen als Anhaltspunkt für den Entwurf des Sentinel-Systems. Im Allgemeinen basieren entwurfsbezogene Empfehlungen auf dem Ereignisratenbereich. Diese Empfehlungen basieren jedoch auf folgenden Annahmen:

- Die Ereignisrate liegt im oberen Drittel des EPS-Bereichs.
- Die durchschnittliche Ereignisgröße beträgt 600 Byte.
- Alle Ereignisse werden in der Datenbank gespeichert (es gibt also keine Filter zum Verwerfen von Ereignissen).
- Daten werden 30 Tagen lang online in der Datenbank gespeichert.
- Der Speicherplatz für Advisor-Daten ist in den Spezifikationen in den nachfolgenden Tabellen nicht berücksichtigt.
- Auf dem Sentinel-Server stehen standardmäßig 5 GB Speicherplatz für das vorübergehende Caching von Ereignisdaten zur Verfügung, die nicht in die Datenbank eingefügt werden können.
- Auf dem Sentinel-Server stehen zudem standardmäßig 5 GB Speicherplatz für Ereignisse zur Verfügung, die nicht in Ereigniserstellungsdateien geschrieben werden können.

  Hinweis: Für das optionale Advisor-Abonnement sind zusätzlich 50 GB Speicherplatz auf dem Datenbankserver erforderlich.

Die Hardware-Empfehlungen für eine Sentinel-Implementierung können basierend auf der jeweiligen Implementierung variieren. Es empfiehlt sich also vor Abschluss der Sentinel-Architektur, Novell Consulting Services zurate zu ziehen. Die nachfolgenden Empfehlungen dienen als Anhaltspunkt.

Hinweis: Aufgrund hohen Ereignisaufkommens und umfangreichem lokalem Caching muss der Sentinel-Server mit Data Access Server (DAS) über ein lokales oder freigegebenes Disk-Array mit Striping-Funktionalität (RAID) mit mindestens 4 Datenträger-Spindles verfügen.

Die verteilten Hosts müssen über einen einzigen Hochgeschwindigkeits-Switch (GIGE) mit den anderen Sentinel-Server-Hosts verbunden sein, um Engpässe beim Netzwerkdatenverkehr zu vermeiden.

Novell empfiehlt, Crystal Reports Server auf einem eigenen dedizierten Computer zu installieren, insbesondere, wenn die Datenbank groß ist bzw. die Berichtsfunktion häufig genutzt wird. Crystal kann auf demselben Computer wie die Datenbank installiert werden, wenn die Datenbank klein ist, die Berichtsfunktion selten genutzt wird und die Datenbank entweder unter Windows oder Linux (nicht Solaris) installiert wurde. Bei den nachfolgend aufgeführten empfohlenen Konfigurationen handelt es sich um kleine, mittlere und große Implementierungen, die jedoch auf Sentinel 5.1.3. basieren. Nach Abschluss der Testphase werden auf der Website zur Novell-Dokumentation unter http://www.novell.com/documentation/sentinel61 (http://www.novell.com/documentation/sentinel61) aktualisierte Empfehlungen veröffentlicht.

Tabelle 2-4 *Konfiguration mit zwei Computern, für EPS von 1-500*

EPS von 1-500: Konfiguration mit zwei Computern			
Komponenten	**RAM**	**Speicherplatz**	**Prozessor**
Computer 1: Sentinel-Server/ Collector Manager ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor ◆ Collector Manager/Collectors ◆ Datenbank ◆ Crystal Reports Server (optional für Windows/Linux)	6 GB	300 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5150 (2,66 GHz) oder Sun Solaris – 4 x UltraSPARC IIIi (1,5 GHz)
Computer 2: Berichtsserver ◆ Crystal Reports Server	2 GB	20 GB	Windows oder Linux – 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

Tabelle 2-5 *Konfiguration mit drei Computern, bei EPS von 500-1500*

EPS von 500-1500: Konfiguration mit drei Computern			
Komponenten	**RAM**	**Speicherplatz**	**Prozessor**
Computer 1: Sentinel-Server/Collector Manager ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor ◆ Collector Manager/Collectors	4 GB	90 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+

EPS von 500-1500: Konfiguration mit drei Computern			
Komponenten	**RAM**	**Speicherplatz**	**Prozessor**
Computer 2: Datenbank ◆ Datenbank ◆ Crystal Reports Server (optional für Windows/Linux)	4 GB+	1 TB+	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 3: Berichtsserver (nur erforderlich, wenn Sentinel/DB unter Solaris) ◆ Crystal Reports Server	2 GB	20 GB	Windows oder Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

Tabelle 2-6 *Konfiguration mit 4-5 Computern, für EPS von 1500-3000*

EPS von 1500-3000: Konfiguration mit 4-5 Computern			
Komponenten	**RAM**	**Speicherplatz**	**Prozessor**
Computer 1: Sentinel-Server ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor	4 GB	90 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 2: Datenbank ◆ Datenbank ◆ Crystal Reports Server (optional für Windows/Linux)	8 GB+	3 TB+	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 3: Collector Manager ◆ Collector Manager/ CollectCollectors	2 GB	20 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 4: Berichtsserver ◆ Crystal Reports Server	4 GB	20 GB	Windows oder Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)
Computer 5: Weitere Instanz von DAS_Binary (erforderlich bei EPS > 2000) Anweisungen zur Konfiguration finden Sie in Kapitel 6, „Hinzufügen von Sentinel-Komponenten“, auf Seite 87..	2 GB	40 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+

Installieren von Sentinel 6.1

3

- Abschnitt 3.1, „Übersicht über Installationsprogramm“, auf Seite 31
- Abschnitt 3.2, „Sentinel-Konfigurationen“, auf Seite 32
- Abschnitt 3.3, „Allgemeine Voraussetzungen für die Installation“, auf Seite 34
- Abschnitt 3.4, „Datenbankinstallation“, auf Seite 39
- Abschnitt 3.5, „Einfache Installation“, auf Seite 43
- Abschnitt 3.6, „Benutzerdefinierte Installation“, auf Seite 46
- Abschnitt 3.7, „Installation von Sentinel als Domänenbenutzer“, auf Seite 59
- Abschnitt 3.8, „Konfiguration nach der Installation“, auf Seite 59

3.1 Übersicht über Installationsprogramm

Dieser Abschnitt enthält hilfreiche Hinweise zur Installation der Hauptkomponenten des Sentinel-Systems. Im Sentinel-Installationsprogramm können Sie zwischen der einfachen und der benutzerdefinierten Installation wählen. Bei der einfachen Installation werden alle Komponenten auf einem Computer installiert; sie ist für Demonstrations- oder Schulungssysteme vorgesehen. Da bei der einfachen Installation zahlreiche Minimal-Standardeinstellungen verwendet werden, ist sie für Produktionsumgebungen ungeeignet. Mithilfe der benutzerdefinierten Installation können eine oder mehrere Sentinel-Komponenten gleichzeitig installiert werden. Sie ist für verteilte Produktionsinstallationen vorgesehen.

Neben den Sentinel-Komponenten kann das Sentinel-System verschiedene weitere Anwendungen umfassen:

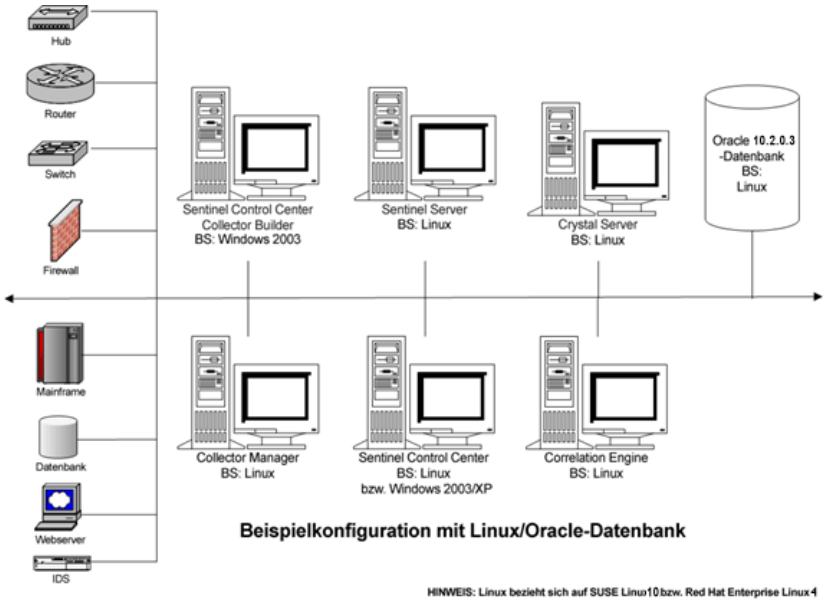
- **Datenbank:** Die Datenbank, in der Ereignisse, korrelierte Ereignisse sowie Konfigurationsinformationen gespeichert werden, ist essenzieller Bestandteil des Sentinel-Systems. Installieren Sie die Datenbank entsprechend der von Oracle und Microsoft empfohlenen Best Practices für Datenbankinstallationen, Verzeichnisstruktur usw.
- **Crystal Reports Server:** Crystal (und der zugehörige Webserver/die zugehörige Datenbank) dient der Ausführung von Berichten aus der Berichtsbibliothek von Novell bzw. von individuell gestalteten Berichten. Für Crystal-Komponenten gibt es ein gesondertes Installationsprogramm. Weitere Informationen zur Installation von Crystal finden Sie in den Abschnitten Kapitel 8, „Crystal Reports für Windows“, auf Seite 101 und Kapitel 9, „Crystal Reports für Linux“, auf Seite 131.
- **Crystal Reports Developer:** Mit dieser Anwendung werden Berichte erstellt und bearbeitet.
- **Advisor:** Advisor stellt Echtzeit-Daten zu Angriffen und Anfälligkeiten bereit; dies schließt die Schwachstellenerkennung ein, die dazu dient, zu ermitteln, welchen Bedrohungen anfällige Systeme ausgesetzt sind. Hierbei handelt es sich um ein optionales Modul. Weitere Informationen zu Advisor sowie Informationen zum Installationsprogramm für den Advisor Core Data-Snapshot finden Sie unter Kapitel 4, „Advisor-Konfiguration“, auf Seite 65.
- **Drittanbieter-Integration:** Sentinel kann in HP OpenView Service Desk integriert werden.

Hinweis: Früher war die Remedy Service Desk-Integration als Installationsoption verfügbar. In Sentinel 6.1 wird Remedy Integration mithilfe eines Integrator-Plugins erreicht und ist nicht mehr Teil des Sentinel-Installationsprogramms. Wenn Sie über die entsprechende Lizenz verfügen, können Sie Remedy Integrator und die dazugehörige Aktion von der Inhalts-Website unter http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html) herunterladen.

3.2 Sentinel-Konfigurationen

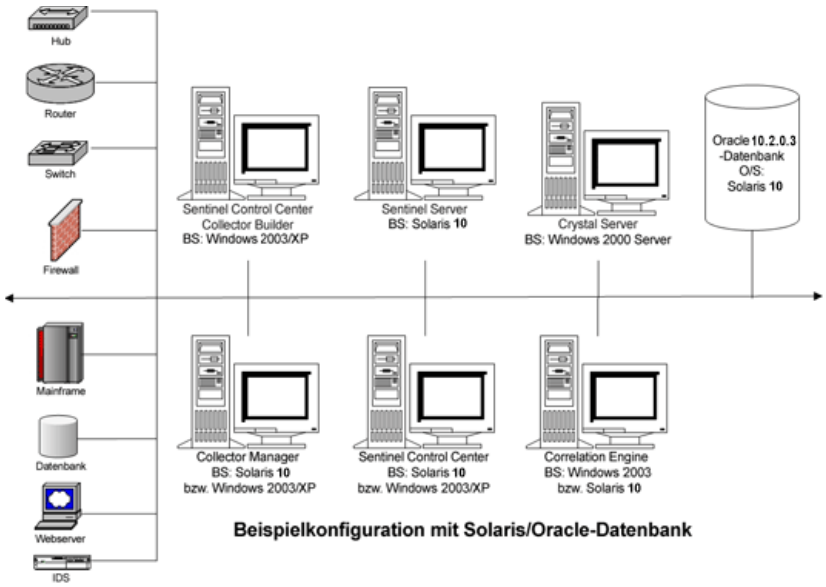
Nachfolgend sind einige typische Konfigurationen für Sentinel aufgeführt. Unter Linux

Abbildung 3-1 *Sentinel-Konfigurationen unter Linux*



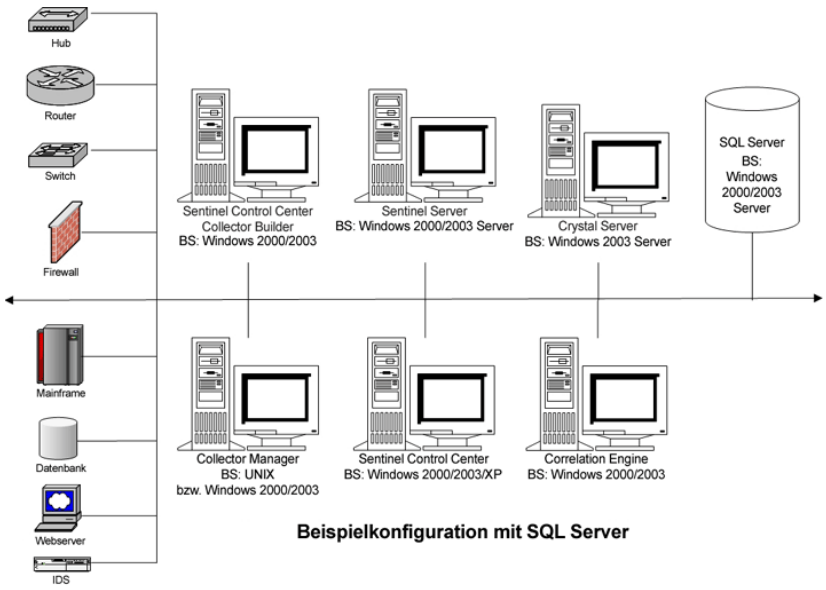
3.2.1 Unter Solaris

Abbildung 3-2 *Sentinel-Konfigurationen unter Solaris*



3.2.2 Unter Windows

Abbildung 3-3 *Sentinel-Konfigurationen unter Windows*



3.3 Allgemeine Voraussetzungen für die Installation

Nachfolgend sind mehrere Schritte aufgeführt, die vor der Installation von Sentinel durchgeführt werden sollen. Weitere Informationen zu zahlreichen dieser Voraussetzungen (einschließlich der Liste mit zertifizierten Plattformen) finden Sie hier: Kapitel 2, „Systemanforderungen“, auf Seite 21.

- Vergewissern Sie sich, dass sämtliche Computer in der Sentinel-Architektur die Mindestsystemanforderungen erfüllen.
- Vergewissern Sie sich, dass es sich bei den Betriebssystemen für sämtliche Komponenten des Systems um zertifizierte Plattformen handelt und dass das Betriebssystem mithilfe aktueller bewährter sicherheitsbezogener Vorgehensweisen „verstärkt“ wurde.
- Vergewissern Sie sich bei der Installation unter SUSE Linux Enterprise Server 10, dass SLES das ext3-Dateisystem verwendet.
- Vergewissern Sie sich bei der Installation des Collector Managers auf einem 64-Bit-Computer, dass 32-Bit-Bibliotheken verfügbar sind. Die 32-Bit-Bibliotheken sind erforderlich, wenn ein Collector ausgeführt wird, der in der proprietären Collector-Sprache geschrieben wurde (dies trifft auf nahezu alle vor Juni 2008 geschriebenen Collectors zu), bzw. wenn bestimmte Connectors ausgeführt werden (etwa der LEA-Connector). Auf JavaScript basierende Collectors sowie der Rest von Sentinel sind 64-Bit-fähig. Sicherzustellen, dass diese Bibliotheken verfügbar sind, ist besonders auf Linux-Plattformen wichtig, die sie möglicherweise nicht standardmäßig enthalten.
- Vor der Installation von Sentinel 6.1 müssen Sie das SUNWxcu4-Paket auf Ihrem Solaris-Computer installieren.
- Vergewissern Sie sich, dass eine Sentinel-zertifizierte Datenbank installiert ist. (Wenn Sie mit Oracle arbeiten, ist die Enterprise Edition mit Partitionierung erforderlich, da das Datenarchiv anderenfalls nicht verwendet werden kann.) Weitere Informationen zu zertifizierten Versionen finden Sie hier: Kapitel 2, „Systemanforderungen“, auf Seite 21.
- Im Novell Customer Center (https://secure-www.novell.com/center/regadmin) finden Sie Seriennummern und Lizenzschlüssel von Sentinel, Crystal Reports Server und Crystal Reports Developer. Wenn Sie den optionalen Advisor-Datenfeed zur Schwachstellenerkennung erworben haben, vergewissern Sie sich in Customer Center, dass dieses Datenabonnement gemeinsam mit dem Rest Ihrer Novell-Produkte aufgeführt wird.
- Installieren und konfigurieren Sie einen SMTP-(Simple Mail Transfer Protocol-)Server, wenn Sie Email-Benachrichtigungen über das Sentinel-System senden möchten.
- Erstellen Sie ein Verzeichnis, dessen Name nur aus ASCII-(American Standard Code for Information Interchange-)Zeichen besteht (keine Sonderzeichen), von dem aus das Installationsprogramm ausgeführt werden soll.
- Vergeben Sie Hauptbenutzer-Privilegien an „Domänenbenutzer“.

Vollständige Sentinel-Installationen müssen immer auf einem „sauberen“ System durchgeführt werden. War Sentinel 6 zuvor auf einem oder mehreren Computern installiert, empfiehlt Novell, die Deinstallationsanweisungen in Kapitel 10, „Deinstallieren von Sentinel“, auf Seite 147 zu befolgen. Informationen zur Deinstallation von Vorgängerversionen von Sentinel finden Sie in den entsprechenden Installationshandbüchern auf der Website zur Novell-Dokumentation (http://www.novell.com/documentation/).

Hinweis: Eine Anleitung für ein Upgrade von einer früheren Version von Sentinel 6 auf Sentinel 6.1 ist im Patch-Installationsprogramm enthalten.

3.3.1 Erteilen von Hauptbenutzer-Privilegien für „Domänenbenutzer“

Wichtig: Wenn Sie Sentinel als Domänenbenutzer installieren (der Benutzer also auf dem Active Directory-Computer und dem lokalen Computer kein Mitglied der Administratorgruppe ist), sollte der Domänenbenutzer zum Starten der Sentinel-Services Hauptbenutzer sein.

So erteilen Sie Domänenbenutzern Hauptbenutzer-Privilegien:

1. Klicken Sie mit der rechten Maustaste auf „Arbeitsplatz“ und wählen Sie „Verwalten“.
2. Wählen Sie im Fenster „Computerverwaltung“ die Optionsfolge „Lokale Benutzer und Gruppen“ > „Gruppen“.
3. Doppelklicken Sie auf „Hauptbenutzer“ und fügen Sie den Domänenbenutzer im Format „domäne/domänenbenutzer“ dem lokalen System hinzu, auf dem Sentinel mit dieser Identität installiert ist.

3.3.2 Voraussetzungen für die Sentinel-Datenbankinstallation

Vor der Installation der Sentinel-Datenbankkomponenten müssen die nachfolgend aufgeführten Schritte durchgeführt und die nachfolgend aufgeführten Informationen zusammengetragen werden.

Voraussetzungen für die Linux-/Solaris-Datenbankinstallation für Sentinel

- Erfolgt die Installation unter SLES 10, muss „ext3“ das Dateisystem des Betriebssystems sein.
- Unter Linux/Solaris muss die Oracle-Datenbank installiert sein und ausgeführt werden.
- Unter Linux/Solaris muss der Oracle-JDBC-(Java Database Connectivity-)Client (`ojdbc14.jar`) auf dem Computer installiert werden, von dem aus Sie das Installationsprogramm ausführen. Wenn Sie das Sentinel-Installationsprogramm auf dem Datenbankcomputer ausführen, sollte vom Datenbank-Installationsprogramm bereits ein kompatibler JDBC-Client installiert worden sein. Wenn Sie das Sentinel-Installationsprogramm auf einem anderen Computer ausführen, müssen die Datenbankinstanz manuell erstellt und der kompatible JDBC-Client manuell auf dem Computer installiert werden (mit dem Installationsprogramm). Obwohl neuere Oracle-Treiber abwärtskompatibel sein sollten, wurden Sentinel-Tests mit den Treibern durchgeführt, die im Lieferumfang der Oracle-Datenbank enthalten waren (es wurden beispielsweise 10.2.0.3-Treiber mit der 10.2.0.3-Datenbank getestet).

  Hinweis: Sentinel kann die Oracle 10-Datenbank aufgrund von Fehlern in den Oracle-Skripts `dbstart` und `dbshut` nicht aufrufen. Sie müssen die Skripts `dbstart` und `dbshut` nach der Installation von Sentinel bearbeiten. Weitere Informationen zum Bearbeiten dieser Skripts finden Sie unter Abschnitt 3.8.7, „Bearbeiten der Oracle-Skripts „dbstart“ und „dbshut““, auf Seite 62.

Hinweis: Für optimale Leistung wird Folgendes dringend empfohlen: Wenn Sie die Installation in RAID (Redundant Array of Independent Disks) durchführen und Ihre RAID-Umgebung dies zulässt, konfigurieren Sie das System so, dass das Transaktionsprotokoll auf den Datenträger mit der höchsten Schreibgeschwindigkeit verweist, d.h. einen separaten physischen Datenträger, auf dem die Datenbankdateien gespeichert sind.

- Es wird empfohlen, zuzulassen, dass das Sentinel-Installationsprogramm die Oracle-Datenbankinstanz für Sentinel erstellt.
- Falls gewünscht, kann die Erstellung der Datenbankinstanz manuell durchgeführt werden. Informationen, wie Sie sicherstellen, dass diese Instanz mit Sentinel kompatibel ist, erhalten Sie unter Abschnitt B.2, „Manuelle Oracle-Instanzerstellung (optional)“, auf Seite 163. Wenn Sie sich für diese Option entscheiden, müssen Sie das von Novell bereitgestellte Skript `createEsecDBA.sh` ausführen, um mithilfe des Sentinel-Installationsprogramms die Datenbankobjekte der manuell erstellten Oracle-Datenbankinstanz hinzuzufügen. Weitere Informationen finden Sie unter Abschnitt 3.6, „Benutzerdefinierte Installation“, auf Seite 46.

Hinweis: Wenn Sie eine bestehende oder manuell erstellte Oracle-Datenbankinstanz verwenden, muss sie abgesehen vom Sentinel-Datenbankbenutzer leer sein.

- Ermitteln Sie die Anmeldeberechtigung für den Benutzer des Oracle-Betriebssystems (Standard: oracle).
- Ermitteln Sie die Anmeldeberechtigung für SYSTEM und SYS.
- Vergewissern Sie sich, dass die folgenden Umgebungsvariablen für den Oracle-Betriebssystembenutzer festgelegt wurden:
  - ORACLE_HOME (bei echo $ORACLE_HOME wird z. B. möglicherweise /opt/oracle/product/10gR2/db zurückgegeben)
  - ORACLE_BASE (bei echo $ORACLE_BASE wird z. B. /opt/oracle zurückgegeben)
  - PATH (muss $ORACLE_HOME/bin enthalten)
- Bestimmen Sie eine entsprechende Oracle-Listener-Port-Nummer (Standard: 1521).
- Erstellen Sie unter Linux/Solaris Verzeichnisse für folgende Speicherorte:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis
  - Temporäres Verzeichnis und Verzeichnis zum Rückgängigmachen
  - Verzeichnis für Redo-Protokollmitglied A
  - Verzeichnis für Redo-Protokollmitglied B
  - Archivverzeichnis

Hinweis: Der Oracle-Benutzer muss über eine Schreibberechtigung für diese Verzeichnisse verfügen. Um dem Oracle-Benutzer eine Schreibberechtigung für diese Verzeichnisse zu gewähren, führen Sie als Benutzer „root“ folgende Befehle für die einzelnen Verzeichnisse aus:

chown –R oracle:dba <Verzeichnispfad>

chmod –R 770 <Verzeichnispfad>

- Nach der Installation der Sentinel-Datenbank unter Oracle enthält die Datenbank folgende Benutzer:
- **esecdba:** Eigentümer des Datenbankschemas. Das Database Administrator-(DBA-)Privileg wird dem Sentinel-Datenbankbenutzer aufgrund von Sicherheitsbedenken nicht gewährt. Um also mit Enterprise Manager arbeiten zu können, müssen Sie einen Benutzer mit DBA-Privilegien erstellen.
- **esecapp:** Datenbankanwendungsbenutzer. Das ist der Anwendungsbenutzer für die Verbindung mit der Datenbank.
- **esecadm:** Hierbei handelt es sich um den Datenbankbenutzer, der der Sentinel-Administrator ist. Dieses Benutzerkonto ist nicht mit dem Sentinel Administrator-Betriebssystembenutzer identisch.
- **esecrpt:** Datenbankreport-Benutzer
- **SYS:** SYS-Datenbankbenutzer
- **SYSTEM:** SYSTEM-Datenbankbenutzer

Voraussetzungen für die Windows-Datenbankinstallation für Sentinel

- Die SQL Server-Datenbank muss installiert sein und ausgeführt werden.
- Der sc-Befehl zum Starten des SQL Server Agent-Service muss im Datenbankbetriebssystem zur Verfügung stehen. (Anderenfalls muss der SQL Server Agent-Service manuell gestartet werden, um die ordnungsgemäße Funktion von Partitionierung und Datenarchivierung zu gewährleisten. Außerdem muss der Service so konfiguriert sein, dass er nach einem durch ein anderes Dienstprogramm veranlassten Systemneustart ebenfalls neu gestartet wird.)
- Ermitteln Sie die Anmeldeberechtigung für den Systemadministrator-Datenbankbenutzer.
  - Wenn die Datenbank die SQL-Authentifizierung zulässt, ist „sa“ der Standarddatenbankadministrator.
  - Befindet sich die Datenbank im reinen Windows-Authentifizierungs-Modus, müssen Sie das Installationsprogramm ausführen, wenn Sie als Systemadministrator-Datenbankbenutzer bei Windows angemeldet sind.
- Legen Sie fest, dass der MSSQLSERVER-Service zur Anmeldung das lokale Systemkonto nutzt.
- Ermitteln Sie gegebenenfalls den Namen der SQL Server-Instanz.

  Hinweis: Sofern Sie Ihre Instanz während der Installation von SQL Server benannt haben, verwenden Sie diesen Namen, wenn Sie während der Installation der Sentinel-Datenbank und/oder der DAS-Komponenten zur Eingabe des Namens der SQL Server-Instanz aufgefordert werden. Wenn Sie bei der SQL Server-Installation keinen Namen für die Instanz vergeben haben, geben Sie bei der Installation keinen Instanzennamen an (fügen Sie also dem Datenbank-Hostnamen nicht „\<instance_name>“ hinzu).

- Erstellen Sie Verzeichnisse für folgende Speicherorte:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis

- Protokollverzeichnis
- Archivverzeichnis

- Bestimmen Sie die Port-Nummer der SQL Server-Instanz (Standard: 1433).

Das Sentinel-System verwendet mehrere Konten für Installation und Systembetrieb. Diese Konten sind in der Sentinel-Datenbank vorhanden und nutzen unter Umständen die SQL Server- oder Windows-Authentifizierung. Wenn bei der Sentinel-Installation die Windows-Authentifizierung für einen oder mehrere Sentinel-Benutzer verwendet werden soll, muss der entsprechende Windows-Domänenbenutzer bereits vor der Installation der Sentinel-Datenbank vorhanden sein.

Der Domänenbenutzer sollte zum Starten von Sentinel-Services über „Hauptbenutzer“-Privilegien verfügen. Weitere Informationen finden Sie unter Abschnitt 3.3.1, „Erteilen von Hauptbenutzer-Privilegien für „Domänenbenutzer““, auf Seite 35.

Folgende Sentinel-Benutzer können einem Windows-Domänenbenutzer zugewiesen werden:

- Sentinel-Datenbankadministrator, der als Schemaeigentümer verwendet wird (hat bei Nutzung der SQL-Authentifizierung standardmäßig den Namen „esecdba“; bei Nutzung der Windows-Authentifizierung kann es sich um ein beliebiges Domänenkonto handeln)
- Sentinel-Anwendungsbenutzer, der von Sentinel-Anwendungen zum Verbindungsaufbau mit der Datenbank verwendet wird (hat bei Nutzung der SQL-Authentifizierung standardmäßig den Namen „esecapp“; bei Nutzung der Windows-Authentifizierung kann es sich um ein beliebiges Domänenkonto handeln)
- Sentinel-Administrator, der als Administrator für die Anmeldung beim Sentinel Control Center verwendet wird (hat bei Nutzung der SQL-Authentifizierung standardmäßig den Namen „esecadm“; bei Nutzung der Windows-Authentifizierung kann es sich um ein beliebiges Domänenkonto handeln)
- Sentinel Report-Benutzer, der zum Erstellen von Berichten verwendet wird (hat bei Nutzung der SQL-Authentifizierung standardmäßig den Namen „esecrpt“; bei Nutzung der Windows-Authentifizierung kann es sich um ein beliebiges Domänenkonto handeln)

Hinweis: Der Sentinel-Datebankadministratorbenutzer, der Sentinel-Anwendungsbenutzer und der Sentinel-Administratorbenutzer sind in der Datenbank standardmäßig vorhanden.

Sentinel unterstützt weder Microsoft-Clustering noch Hochverfügbarkeit für Windows.

Nach der Installation der Sentinel-Datenbank unter SQL Server unter Verwendung der lokalen Authentifizierung enthält die Datenbank folgende Benutzer:

- **esecdba:** Eigentümer des Datenbankschemas. Das Database Administrator-(DBA-)Privileg wird dem Sentinel-Datenbankbenutzer aufgrund von Sicherheitsbedenken nicht gewährt. Um also mit Enterprise Manager arbeiten zu können, müssen Sie einen Benutzer mit DBA-Privilegien erstellen.
- **esecapp:** Datenbankanwendungsbenutzer. Das ist der Anwendungsbenutzer für die Verbindung mit der Datenbank.
- **esecadm:** Hierbei handelt es sich um den Datenbankbenutzer, der der Sentinel-Administrator ist. Dieses Benutzerkonto ist nicht mit dem Sentinel Administrator-Betriebssystembenutzer identisch.
- **esecrpt:** Datenbankreport-Benutzer
- **sa:** Systemadministrator-Datenbankbenutzer

3.3.3 Einstellungen des Authentifizierungsmodus unter Microsoft SQL

Unter Windows müssen Sie SQL Server im gemischten Authentifizierungsmodus installieren, um sich über die Windows- bzw. SQL Server-Authentifizierung beim Sentinel Control Center anmelden zu können. Wenn Sie SQL Server über die Windows-Authentifizierung installieren, ist die Anmeldung lediglich über die Windows-Authentifizierung möglich.

So bearbeiten Sie die Einstellungen für den Authentifizierungsmodus:

1. Klicken Sie in Microsoft SQL Server Management Studio mit der rechten Maustaste auf den Server, dessen Einstellungen Sie bearbeiten möchten.
2. Wählen Sie „Eigenschaften“ aus und klicken Sie dann auf die Option für die Sicherheit.
3. Wählen Sie im Bereich für den SQL Server- und Windows-Authentifizierungsmodus bzw. für den Windows-Authentifizierungsmodus die zutreffende Authentifizierungsoption aus.

3.3.4 Voraussetzungen für die Sentinel-Serverinstallation

Wenn Sie die Sentinel-Datenbank nicht auf dem gleichen Computer wie den Sentinel-Server installieren, müssen Sie die Sentinel-Datenbank vor den anderen Sentinel-Komponenten installieren.

3.3.5 Voraussetzungen für die Advisor-Installation

Um Advisor installieren zu können, müssen Sie das optionale Sentinel Exploit Detection and Advisor Data-Abonnement (für die Sentinel-Schwachstellenerkennung und Advisor-Daten) erwerben. Ist diese Voraussetzung erfüllt, können Sie mit Ihren Novell eLogin-Daten die Advisor-Daten herunterladen und aktualisieren.

Wenn Sie die Option „Direktes Herunterladen vom Internet“ wählen, sollte der ausgehende Port 443 offen sein. Sie sollten die Installation von Crystal Reports Server-Software auf Ihrem System einplanen, um die Ausführung von Berichten zu ermöglichen.

Hinweis: Wenn Sie beabsichtigen, Advisor lediglich für die Schwachstellenerkennung zu nutzen, ist die Installation von Crystal Reports Server-Software nicht erforderlich. Weitere Informationen zur Vorgehensweise bei der Installation finden Sie unter Kapitel 4, „Advisor-Konfiguration“, auf Seite 65.

3.4 Datenbankinstallation

Für die Installation von Oracle bzw. SQL Server sollte ein erfahrener Datenbankadministrator (DBA) herangezogen werden. Neben den Empfehlungen des DBA sind auch die Empfehlungen von Novell in Bezug auf die Installation von Oracle hilfreich. Diese Empfehlungen beziehen sich auf folgende Bereiche:

- Festlegen von Kernel-Werten
- Unter Solaris und RHEL 4:
  - Erstellen eines Gruppen- und Benutzerkontos für Oracle

- Festlegen der Umgebungsvariablen
- Prüfen des Solaris-Layouts

- Installation von Oracle
- Aufrüsten auf Oracle mit Patches (falls erforderlich)

3.4.1 Festlegen von Kernel-Werten

Warnung: GEWÄHRLEISTUNGSAUSSCHLUSS: Bei den in diesem Abschnitt empfohlenen Kernel-Werten handelt es sich ausschließlich um Mindestwerte. Diese Einstellungen sollten nur geändert werden, wenn Ihre Systemeinstellungen unterhalb der empfohlenen Mindestwerte liegen, und nur nach Zurateziehen Ihres Systemadministrators und der Oracle-Dokumentation.

So legen Sie die Kernel-Werte unter Linux fest:

1. Melden Sie sich als Root an.
2. Erstellen Sie eine Sicherungskopie von `/etc/sysctl.conf`.
3. Ändern Sie in einem Texteditor die Kernel-Parameter, indem Sie folgenden Text am Ende der Datei `/etc/sysctl.conf` anfügen:

   Hinweis: Bei den nachfolgenden Kernel-Einstellungen handelt es sich um empfohlene Mindesteinstellungen. Diese Einstellungen können auf einen höheren Wert eingestellt werden, wenn die Hardware dies zulässt.

   Zum Festlegen der aktuellen Einstellung für einen bestimmten Kernel-Parameter führen Sie folgenden Befehl aus:

   ```
   sysctl <kernel_parameter>
   ```

   Beispiel: Zum Überprüfen des aktuellen Werts des Kernel-Parameters „kernel.sem“ führen Sie folgenden Befehl aus: `sysctl kernel.sem`.

   Nur unter SUSE LINUX 10 SP2:

   ```
   # Oracle requires MLOCK privilege for hugetlb memory.
   vm.disable_cap_mlock=1
   ```

   Info zu REDHAT LINUX 4

   ```
   # Kernel settings for Oracle
   kernel.core_uses_pid = 1
   kernel.shmall = 2097152
   kernel.shmmax = 2147483648
   kernel.shmmni = 4096
   kernel.sem = 250 32000 100 128
   fs.file-max = 65536
   net.ipv4.ip_local_port_range = 1024 65000
   net.core.rmem_default = 262144
   net.core.rmem_max = 262144
   net.core.wmem_default = 262144
   net.core.wmem_max = 262144
   ```

4. Führen Sie den folgenden Befehl aus, damit die Änderungen in der Datei `/etc/sysctl.conf` geladen werden:

```
sysctl -p
/sbin/sysctl -p (on RedHat Linux4)
```

5 Legen Sie die Datei-Handles und Prozesslimits fest, indem Sie den folgenden Text an das Ende der Datei `/etc/security/limits.conf` anhängen. „nproc“ ist die Obergrenze der Anzahl an Prozessen und „nofile“ ist die Obergrenze der Anzahl geöffneter Dateien. Das sind die empfohlenen Werte, aber sie können bei Bedarf geändert werden. Im folgenden Text wird angenommen, dass Ihre Oracle-Benutzer-ID „oracle“ lautet.

```
# Settings added for Oracle
oracle          soft    nofile  65536
oracle          hard    nofile  65536
oracle          soft    nproc   16384
oracle          hard    nproc   16384
```

So legen Sie die Kernel-Werte unter Solaris 10 fest:

Für Oracle 10g:

noexec_user_stack=1	semsys:seminfo_semvmx=32767
semsys:seminfo_semmni=100	shmsys:shminfo_shmmax=4294967295
semsys:seminfo_semmns=1024	shmsys:shminfo_shmmni=100
semsys:seminfo_semmsl=256	

1 Standardmäßig werden Oracle-Instanzen als Oracle-Benutzer der Gruppe „dba“ ausgeführt. Ein Projekt mit dem Namen `group.dba` wird als Standardprojekt für den Oracle-Benutzer erstellt. Führen Sie den Befehl „id“ aus, um das Standardprojekt für den Oracle-Benutzer zu überprüfen.

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ exit
```

2 Um die Obergrenze für den gemeinsam genutzten Arbeitsspeicher auf 2 GB zu setzen, führen Sie den Befehl „projmod“ aus.

```
# projmod -sK "project.max-shm-memory=(privileged,2G,deny)"
group.dba
```

Alternativ können Sie die Ressourcensteuerung project.max - `shm-memory=(privileged,2147483648,deny)` zum letzten Feld der Projekteinträge für das Oracle-Projekt hinzufügen.

3 Nach Abschluss dieser Schritte sollte die Datei /etc/project Folgendes enthalten:

```
# cat /etc/project
```

4 Hier die Ausgabe des Befehls:

```
system:0::::
user.root:1::::
noproject:2::::
default:3::::
```

```
group.staff:10::::
group.dba:100:Oracle default
project:::project.max-shmmemory=(privileged,2147483648,deny
```

5 Um zu überprüfen, ob die Ressourcensteuerung aktiv ist, führen Sie die Befehle „id“ und „prctl“ aus:

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ prctl -n project.max-shm-memory -i process $$
process: 5754: -bash
NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT
project.max-shm-memory
privileged 2.00GB – deny
```

Hinweis: Weitere Informationen finden Sie in der Oracle-Dokumentation für die Installation von Solaris 10.

3.4.2 Erstellen von Gruppen- und Benutzerkonten für Oracle (nur bei Solaris)

So erstellen Sie ein Benutzer- und ein Gruppenkonto und legen die Umgebungsvariablen fest:

1 Melden Sie sich als „root“ an.

2 Erstellen Sie eine UNIX-Gruppe und UNIX-Benutzerkonten für den Oracle-Datenbankeigentümer.

- Fügen Sie eine dba-Gruppe hinzu (als „root“):
  `groupadd –g 400 dba`
- Fügen Sie den Oracle-Benutzer (als „root“) für die csh-Shell hinzu:
  `useradd –g dba –d /export/home/oracle –m –s /bin/csh oracle`
- Fügen Sie den Oracle-Benutzer (als „root“) für die bash-Shell hinzu:
  `useradd –g dba –d /export/home/oracle –m –s /bin/bash oracle`

3.4.3 Festlegen von Umgebungsvariablen für Oracle (nur bei Solaris)

So legen Sie Umgebungsvariablen fest:

1 Melden Sie sich als „root“ an.

2 Beim Festlegen der erforderlichen Umgebungsvariablen für Oracle in der csh-Shell sollten der Datei `local.cshrc` die folgenden Informationen hinzugefügt werden:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
usr/ucb/etc.)
```

```
if ( $?prompt ) then
set history=32
endif
```

3 Beim Festlegen der erforderlichen Umgebungsvariablen für Oracle in der bash-Shell sollten der Datei `.profile` im Verzeichnis „$ORACLE_HOME“ die folgenden Informationen hinzugefügt werden:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
usr/ucb/etc.)
if ( $?prompt ) then
set history=32
endif
```

3.4.4 Oracle installieren

Informationen zur Durchführung der Oracle-Installation finden Sie in Anhang B, „Oracle-Setup“, auf Seite 159 In diesem Abschnitt werden die für Sentinel-Operationen empfohlenen Installationseinstellungen dargestellt. Außerdem werden die Verfahren zum Erstellen der Oracle-Instanz erläutert. (Novell empfiehlt die Erstellung der Instanz mithilfe des Sentinel-Installationsprogramms, stellt jedoch eine Anleitung für den Fall bereit, dass gemäß den geltenden Unternehmensrichtlinien die manuelle Erstellung der Instanz durch den DBA erforderlich ist.)

3.5 Einfache Installation

Bei der Option „Einfache Installation“ handelt es sich um eine All-in-One-Installationsoption, bei der Sentinel Services, Collector Manager und Sentinel-Anwendungen zusammen mit der Datenbank auf demselben Computer installiert werden. Dieser Installationstyp ist nur zu Demonstrations- und Schulungszwecken gedacht und sollte nicht für Produktionsumgebungen verwendet werden.

Nachdem die Datenbankinstallation durchgeführt wurde und die im vorangehenden Abschnitt angegebenen Anforderungen erfüllt sind, können Sie mit der Installation von Sentinel fortfahren. Bei Auswahl der Option „Einfache Installation“ wird von bestimmten Voraussetzungen ausgegangen und es werden mehrere Standardeinstellungen verwendet:

- Unter Windows ist SQL-Authentifizierung für die SQL Server-Datenbanken zulässig.
- Für den Sentinel-Datenbankadministrator, den Sentinel-Administrator, den Sentinel-Anwendungsbenutzer und den Sentinel Report-Benutzer wird jeweils dasselbe Passwort verwendet.
- Advisor ist für die Verwendung von „Direktes Herunterladen vom Internet“ konfiguriert.
- Advisor ist so eingestellt, dass alle 12 Stunden neue Informationen heruntergeladen werden.
- Advisor-Email-Benachrichtigungen sind aktiviert.
- Die Datenbankgröße beträgt 10 GB.

So installieren Sie Sentinel:

1 Melden Sie sich unter Solaris/Linux als Benutzer „root“ bzw. unter Windows als Administratorbenutzer an.

2 Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.

3 Starten Sie das Installationsprogramm. Wechseln Sie dazu in das Installationsverzeichnis auf der CD-ROM und gehen Sie dann wie folgt vor:

- Unter Windows: Führen Sie `setup.bat` aus.
- Unter Solaris/Linux:

  Für GUI-Modus:

  ```
  ./setup.sh
  ```

  Oder für den textbasierten Modus („serielle Konsole“):

  ```
  ./setup.sh –console
  ```

Hinweis: Sie können das Installationsprogramm unter UNIX nicht über einen Verzeichnispfad ausführen, der Leerzeichen enthält.

4 Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:

Englisch	Italienisch
Französisch	= Portugiesisch (Brasilien)
Deutsch	Spanisch
Chinesisch (Vereinfacht)	Japanisch
Chinesisch (Traditionell)	

5 Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.

6 Lesen Sie die Lizenzvereinbarung durch und erklären Sie Ihr Einverständnis. Klicken Sie anschließend auf "Weiter".

7 Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie anschließend auf "Weiter".

Hinweis: Die Installation kann nicht in einem Verzeichnis erfolgen, dessen Name Sonderzeichen oder Nicht-ASCII-Zeichen enthält. Bei einer Installation von Sentinel 6.1 unter Windows x86-64 beispielsweise ist der Standardpfad „C:\Programme (x86)“. Um die Installation fortsetzen zu können, müssen Sie den Standardpfad so ändern, dass er keine Sonderzeichen enthält.

8 Wählen Sie "Einfach" aus. Klicken Sie anschließend auf "Weiter".

9 Geben Sie in diesem Fenster die Konfigurationsinformationen an und klicken Sie auf „Weiter“.

- Seriennummer
- Lizenzschlüssel
- SMTP-Server
  - Sentinel sendet Emails über diesen Server.
- Email
  - Bei den von Sentinel gesendeten Emails wird diese Email-Adresse als Sender angegeben.
- Globales Systempasswort

- Das hier eingegebene Passwort gilt für alle Standardbenutzer. Dazu gehören sowohl der Sentinel-Administratorbenutzer als auch die Datenbankbenutzer. Weitere Informationen zur Liste der mithilfe der Installation erstellten Standarddatenbankbenutzer finden Sie in Abschnitt 3.8.2, „Sentinel-Datenbank“, auf Seite 60.
- Advisor-Benutzername und Passwort (optional)
  - Zur Installation von Advisor geben Sie den Novell eLogin-Namen und das Passwort für die Advisor-Lizenz an. Geben Sie das Advisor-Passwort ein zweites Mal in das Fenster für die Passwortbestätigung ein.

Hinweis: Benutzernamen und Passwörter, die vor der Verwendung von Sentinel 6.0 SP2 für Advisor galten, sind jetzt ungültig. Sie müssen das mit der Advisor-Lizenz verknüpfte Novell eLogin und Passwort verwenden. In manchen Unternehmen arbeiten mehrere Mitarbeiter mit Novell eLogin-Daten. Sie müssen für die Advisor-Downloads die eLogin-Daten verwenden, die zum Advisor-Kauf gehören.

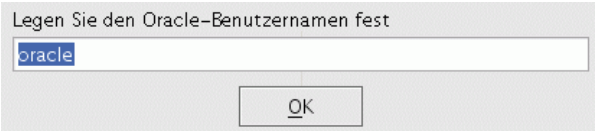
---

10 Zur Datenbankkonfiguration:

- Wählen Sie die Plattform der Zieldatenbank aus.

Unter Solaris/Linux werden Sie zur Eingabe des Oracle-Benutzernamens aufgefordert. Geben sie den Benutzernamen ein und klicken Sie auf „OK“.

Abbildung 3-4 *Feld zur Eingabe des Oracle-Benutzernamens*



Datenbanknamen eingeben

- Unter Linux/Solaris geben Sie die Oracle-JDBC-Treiberdatei an.
- Unter Windows geben Sie den Berechtigungsnachweis für den Datenbankbenutzer und den Namen der SQL Server-Instanz ein.

Klicken Sie anschließend auf "Weiter".

Hinweis: Unter Linux/Solaris sichert das Installationsprogramm alle eventuell bestehenden Dateien vom Typ `tnsnames.ora` und `listener.ora` im Verzeichnis „$ORACLE_HOME/network/admin“. Die Datei `listener.ora` wird mit Verbindungsinformationen für die Sentinel-Datenbank überschrieben und die Datei `tnsnames.ora` wird mit Verbindungsinformationen für die Sentinel-Datenbank ergänzt. Wenn sich weitere Datenbanken auf demselben Server wie die Sentinel-Datenbank befinden, muss der Administrator manuell Informationen aus den gesicherten `listener.ora`-Dateien in der neuen Datei zusammenführen und den Oracle-Listener neu starten, damit andere Anwendungen weiterhin eine Verbindung mit der Datenbank herstellen können.

Abbildung 3-5 *Übersicht über die Datenbankparameter*

Eine MSSQL-Datenbank mit folgenden Parametern wird erstellt:
Die folgende neue Datenbank wird erstellt: ESEC617
Diese Datenbank hat eine Anfangsgröße von 1.000 MB.
Diese Datenbank hat eine maximale Größe von 20000 MB.
Die Speicherorte für die Datendateien lauten wie folgt:
Datendateien: D:\esecdata
Indexdateien: D:\esecdata
Zusammenfassung Datendateien: D:\esecdata
Zusammenfassung Indexdateien: D:\esecdata
Protokolldateien: D:\esecdata
Schemaeigentümer: esecdba
Sentinel-Anwendungsbenutzer: esecapp
Sentinel-Verwalter: esecadm
Sentinel Report-Benutzer: esecrpt

11. Eine Übersicht über die ausgewählten Datenbankparameter wird angezeigt. Klicken Sie anschließend auf "Weiter".
12. Eine Übersicht über die Installation wird angezeigt. Klicken Sie auf "Installieren".
13. Klicken Sie nach der Installation auf „Fertig stellen“.
14. Booten Sie das System neu. (Geplante Services wie das Herunterladen von Advisor können erst nach dem erneuten Booten ausgeführt werden.)

3.6 Benutzerdefinierte Installation

Die Option „Benutzerdefinierte Installation“ ermöglicht eine vollständig verteilte Installation mit größeren Einflussnahmemöglichkeiten auf Arbeitsspeicher und andere Installationseinstellungen. Mit der Option „Benutzerdefinierte Installation“ können auch ein oder mehrere Sentinel-Komponenten installiert werden, darunter:

- Sentinel-Datenbankkomponenten
- Sentinel Services
  - Communication Server
  - Advisor
  - Correlation Engine
  - Data Access Server (DAS)
  - Sentinel Collector Service (Collector Manager)
- Anwendungen
  - Sentinel Control Center
  - Sentinel Data Manager
  - Sentinel Solution Designer
- Drittanbieter-Integration
  - HP OpenView Service Desk

Nachdem die im vorangehenden Abschnitt angegebenen Anforderungen erfüllt sind, können Sie mit der Installation von Sentinel fortfahren.

Die Sentinel-Datenbankkomponenten sollten stets als Erstes installiert werden. Andere Komponenten können gleichzeitig installiert werden, wenn die Systemarchitektur mehrere Komponenten auf dem Datenbankcomputer beinhaltet. Im unten angegebenen Verfahren finden Sie die Schritte zur Installation aller Komponenten auf demselben Computer; eine verteilte Installation beinhaltet eine Teilmenge der unten stehenden Schritte.

So installieren Sie Sentinel:

1. Melden Sie sich unter Solaris/Linux als Benutzer „root“ bzw. unter Windows als Administratorbenutzer an.

   Hinweis: Für eine Installation der Sentinel-Datenbankkomponente unter Windows, wenn sich die Zielinstanz von MS SQL Server im Modus für ausschließliche Windows-Authentifizierung befindet, müssen Sie sich bei Windows als Datenbankbenutzer mit Administratorrechten anmelden.

2. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
3. Starten Sie das Installationsprogramm. Wechseln Sie dazu in das Installationsverzeichnis auf der CD-ROM und gehen Sie dann wie folgt vor:
   - Unter Windows: Führen Sie `setup.bat` aus.
   - Unter Solaris/Linux:

     Für GUI-Modus:

     `./setup.sh`

     Oder für Textmodus („kopflos“):

     `./setup.sh –console`

     Hinweis: Sie können das Installationsprogramm unter UNIX nicht über einen Verzeichnispfad ausführen, der Leerzeichen enthält.

4. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:

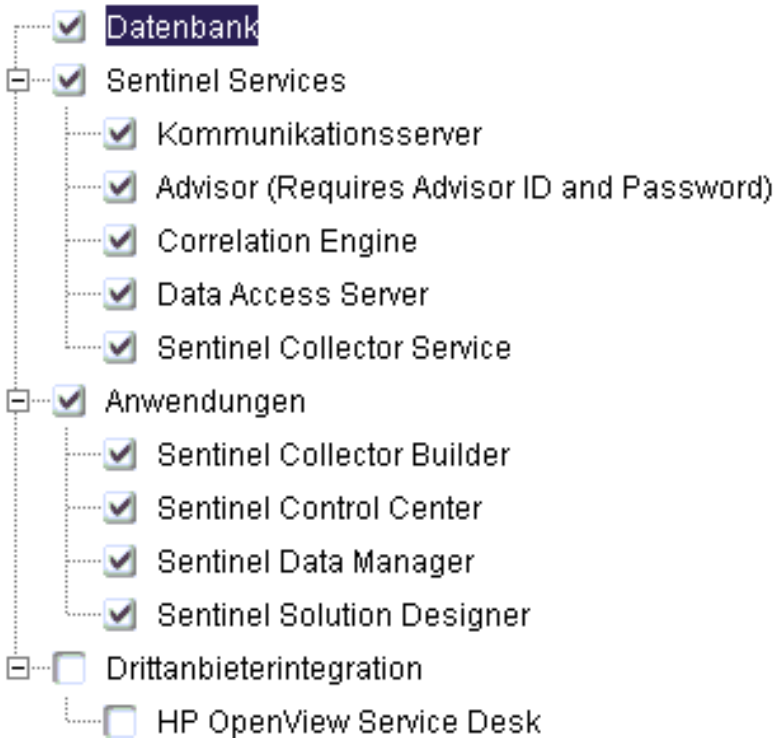
Englisch	Italienisch
Französisch	Portugiesisch (Brasilien)
Deutsch	Spanisch
Chinesisch (Vereinfacht)	Japanisch
Chinesisch (Traditionell)	

5. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.
6. Lesen Sie die Lizenzvereinbarung durch und erklären Sie Ihr Einverständnis. Klicken Sie anschließend auf "Weiter".
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie anschließend auf "Weiter".

   Hinweis: Die Installation kann nicht in einem Verzeichnis erfolgen, das Sonderzeichen oder Nicht-ASCII-Zeichen enthält.

8. Wählen Sie „Benutzerdefiniert“ aus. Klicken Sie anschließend auf "Weiter".

9 Wählen Sie die zu installierenden Sentinel-Komponenten aus.



Folgende Optionen stehen zur Verfügung:

Komponente	Beschreibung
Datenbank	Installiert Sentinel-Datenbankobjekte (Tabellen, Ansichten, gespeicherte Prozeduren usw.) in einer Datenbankinstanz. Optional wird die Datenbankinstanz zuerst erstellt.
Communication Server	Installiert Nachrichten-Bus (iSCALE) und DAS-Proxy
Correlation Engine	Installiert Correlation Engine.
Advisor	Installiert Komponenten, die zum Abonnementservice für Advisor-Daten gehören. Erfordert eine Advisor-Lizenz und muss sich auf demselben Computer befinden wie DAS.
Data Access Server (DAS)	Installiert Komponenten, die mit der Sentinel-Datenbank kommunizieren. Erfordert einen Sentinel-Lizenzschlüssel und eine Seriennummer. (Erforderlich, sofern Advisor installiert wird.)
Sentinel Collector Service	Installiert den Collector Manager, der Verbindungen zu Ereignisquellen, Datenanalyse, Zuordnungen usw. verwaltet.
Sentinel Control Center	Installiert die Hauptkonsole für Sicherheits- oder Konformitätsanalysten.
Sentinel Data Manager (SDM)	Installiert SDM, der für die manuelle Datenbankverwaltung verwendet wird.
Solution Designer	Installiert Solution Designer.

Komponente	Beschreibung
HP OpenView Service Desk	Installiert die Integration mit HP OpenView Service Desk. Erfordert eine Lizenz.

Hinweis: Es tritt eine Zeitverzögerung bei der Schnittstelle auf, wenn Sie eine Komponente auswählen bzw. die Auswahl aufheben.

Hinweis: Wenn keine der untergeordneten Funktionen von Sentinel Services ausgewählt wurde, müssen Sie auch die Funktion Sentinel Services selbst deaktivieren. Sie wird abgeblendet (nicht verfügbar) mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.

Hinweis: Als Teil der Installation der Sentinel-Datenbank legt das Installationsprogramm Dateien im Ordner „%ESEC_HOME%\ unist\db“ ab.

Hinweis: Bei Verwendung des „Konsolen“-Modus werden auf der Komponentenauswahlseite nicht alle Komponenten zusammen angezeigt. Befolgen Sie die Bildschirmanweisungen zur Anzeige und Bearbeitung der ausgewählten untergeordneten Komponenten. Nicht alle untergeordneten Komponenten sind standardmäßig ausgewählt. Informationen hierzu erhalten Sie unterAbschnitt 3.6.1, „Konsoleninstallation unter Linux/Solaris“, auf Seite 57.

10 Wenn Sie auswählen, dass DAS installiert werden soll, werden Sie zur Eingabe folgender Daten aufgefordert:

- Seriennummer
- Lizenzschlüssel

11 Unter Linux/Solaris: Geben Sie den Benutzernamen des Betriebssystem-Sentinel-Administrators ein und den Standort seines Basisverzeichnisses. Das ist der Name des Benutzers, dem das installierte Sentinel-Produkt gehört. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem Basisverzeichnis im angegebenen Verzeichnis erstellt.

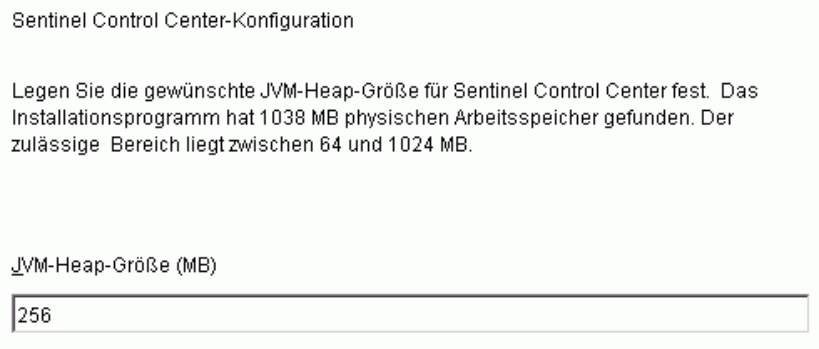
- Benutzername des OS Sentinel-Administrators – Standardmäßig „esecadm“
- Basisverzeichnis des OS Sentinel-Administrators – Standardmäßig „/export/home“. Wenn der Benutzername „esecadm“ lautet, ist das dazugehörige Basisverzeichnis /export/home/esecadm.

Hinweis: So erfüllen Sie die strikten Sicherheitskonfigurationen, die von der allgemeinen Kriterienzertifizierung benötigt werden.

Hinweis: Der Benutzer „esecadm“ wird erstellt, ohne dass ein Passwort festgelegt ist. Um sich als dieser Benutzer anzumelden, müssen Sie zunächst das zugehörige Passwort festlegen.

12 Wenn Sie auswählen, dass Sentinel Control Center installiert werden soll, fordert Sie das Installationsprogramm auf, die maximale Menge an Arbeitsspeicher einzugeben, die Sentinel Control Center zugeordnet werden soll. Geben Sie die maximale JVM-Heap-Größe (MB) an, die ausschließlich von Sentinel Control Center verwendet werden soll.

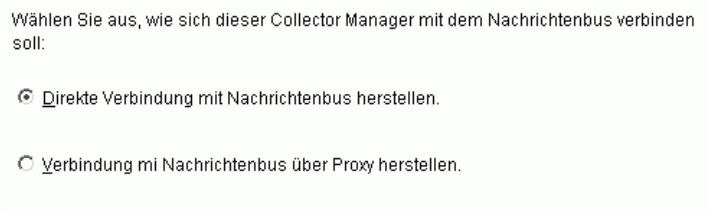
- **JVM-Heap-Größe (MB):** Standardmäßig beträgt dieser Wert 256 MB. Maximal können 1024 MB angegeben werden.


Sentinel Control Center-Konfiguration
Legen Sie die gewünschte JVM-Heap-Größe für Sentinel Control Center fest. Das Installationsprogramm hat 1038 MB physischen Arbeitsspeicher gefunden. Der zulässige Bereich liegt zwischen 64 und 1024 MB.
JVM-Heap-Größe (MB)
256

13 Wenn der Collector Manager für die Installation ausgewählt wurde, Data Access Server (DAS) jedoch nicht, haben Sie zwei Optionen zur Herstellung der Kommunikation zwischen den Sentinel Collector Managers und Sentinel Server. Sie können für den Nachrichten-Bus direkte Kommunikation oder Proxy-Kommunikation auswählen. Weitere Informationen zu diesen beiden Optionen finden Sie hier: Kapitel 7, „Kommunikationsschicht (iSCALE)“, auf Seite 95

Hinweis: Bei Auswahl des Kommunikationstyps „Proxy“ werden Sie unmittelbar nach Abschluss der Installation zur Eingabe der Informationen aufgefordert, die für die Registrierung dieses Collector Managers als verbürgter Client erforderlich sind. Hierfür ist erforderlich, dass der Communication Server ausgeführt wird.

Wenn der Communication Server nicht verfügbar ist, wählen Sie als Kommunikationstyp für den Nachrichten-Bus die direkte Kommunikation aus und konfigurieren Sie später den Kommunikationstyp „Proxy“ manuell, indem Sie Schritt 26 auf Seite 57 (Konfigurieren des Kommunikationstyps „Proxy“) ausführen.


Wählen Sie aus, wie sich dieser Collector Manager mit dem Nachrichtenbus verbinden soll:
Direkte Verbindung mit Nachrichtenbus herstellen.
Verbindung mi Nachrichtenbus über Proxy herstellen.

14 Sie werden aufgefordert, Informationen zu Port/Hostservername für den Communication Server anzugeben. Geben Sie die erforderlichen Informationen ein und klicken Sie auf „Weiter“.

- **Nachrichten-Bus-Port:** der Port, den der Kommunikationsserver überwacht. Die Komponenten, die eine direkte Verbindung mit dem Kommunikationsserver herstellen, verwenden diesen Port.
- **Sentinel Control Center-Proxy-Port:** der Port, den der SSL-Proxyserver (DAS Proxy) überwacht, um mithilfe von Benutzernamen und Passwort authentifizierte Verbindungen zu akzeptieren. Da Sentinel Control Center zur Eingabe von Benutzernamen und Passwort auffordert, verwendet es diesen Port für die Herstellung einer Verbindung mit Sentinel Server.
- **Authentifizierungs-Proxy-Port für das Collector Manager-Zertifikat:** der Port, den der SSL-Proxyserver (DAS Proxy) überwacht, um mithilfe von Zertifikaten authentifizierte Verbindungen zu akzeptieren. Da Sentinel Control Center nicht zur

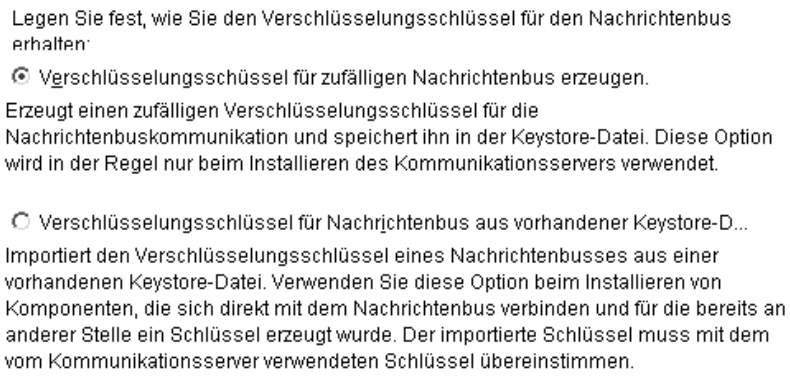
Eingabe von Benutzernamen und Passwort auffordern kann, verwendet es diesen Port für die Herstellung einer Verbindung mit Sentinel Server, wenn es für Verbindungen über den Proxy konfiguiert ist.

Hinweis: Die Portnummern müssen auf allen Computern im Sentinel-System übereinstimmen, damit die Kommunikation möglich ist. Notieren Sie sich diese Ports für spätere Installationen auf anderen Computern.

---

15 Wenn Sie eine Komponente installieren, die eine direkte Verbindung mit dem Nachrichten-Bus herstellt oder wenn Sie Communication Server installieren, werden Sie gefragt, wie der gemeinsam genutzte Verschlüsselungsschlüssel für den Nachrichten-Bus bezogen werden soll.

- Zufallsverschlüsselungsschlüssel generieren
- Verschlüsselungsschlüssel aus keystore-Datei importieren Sie werden aufgefordert, zum Standort einer bestehenden .keystore-Datei zu wechseln.


Legen Sie fest, wie Sie den Verschlüsselungsschlüssel für den Nachrichtenbus erhalten:
Verschlüsselungsschüssel für zufälligen Nachrichtenbus erzeugen.
Erzeugt einen zufälligen Verschlüsselungsschlüssel für die Nachrichtenbuskommunikation und speichert ihn in der Keystore-Datei. Diese Option wird in der Regel nur beim Installieren des Kommunikationsservers verwendet.
Verschlüsselungsschlüssel für Nachrichtenbus aus vorhandener Keystore-D...
Importiert den Verschlüsselungsschlüssel eines Nachrichtenbusses aus einer vorhandenen Keystore-Datei. Verwenden Sie diese Option beim Installieren von Komponenten, die sich direkt mit dem Nachrichtenbus verbinden und für die bereits an anderer Stelle ein Schlüssel erzeugt wurde. Der importierte Schlüssel muss mit dem vom Kommunikationsserver verwendeten Schlüssel übereinstimmen.

Hinweis: Alle Komponenten, die eine direkte Verbindung zum Nachrichten-Bus herstellen, müssen denselben Verschlüsselungsschlüssel verwenden. Novell empfiehlt, während der Installation von Communication Server, einen Zufallsschlüssel für die Verschlüsselung zu generieren und diesen Schlüssel während der Installation von Komponenten auf anderen Computern zu importieren. Komponenten, die die Verbindung über den Proxy herstellen, benötigen den gemeinsam genutzten Verschlüsselungsschlüssel für den Nachrichten-Bus nicht.

Die „.keystore“-Datei wird bei Linux/Solaris unter „$ESEC_HOME/config“ und bei Windows unter „%ESEC_HOME%\config“ abgelegt.

---

16 Wählen Sie die Plattform des Zieldatenbankservers aus. Klicken Sie anschließend auf "Weiter". Wenn Sie ausgewählt haben, dass DAS installiert werden soll und die Sentinel-Datenbankkomponenten bereits installiert sind, werden Sie zur Eingabe der folgenden Informationen für die Sentinel-Datenbank aufgefordert. Diese Informationen werden verwendet, um DAS so zu konfigurieren, dass es auf die Sentinel-Datenbank verweist.

- **Datenbank-Hostname oder IP-Adresse:** Der Name bzw. die IP der bestehenden Sentinel-Datenbank, in der Ereignisse und Konfigurationsinformationen gespeichert werden sollen.
- **Datenbankname:** Der Name der Sentinel-Datenbankinstanz, mit der die DAS-Komponente laut Konfiguration eine Verbindung herstellen soll (Standard: ESEC).

- **Datenbankport:** (Standard - Microsoft SQL Server:1433 und Oracle:1521)
- **Sentinel-Anwendungsdatenbankbenutzer:** Geben Sie den Anmeldenamen für den Sentinel-Anwendungsbenutzer (Standard: „esecapp“) und das Passwort an, das diesem Benutzer während der Installation der Sentinel-Datenbank zugewiesen wurde.

Klicken Sie anschließend auf "Weiter".

17 Wenn Sie ausgewählt haben, dass die Datenbank installiert werden soll, müssen Sie die Datenbank für die Installation konfigurieren:

Unter Windows:

- Wählen Sie Microsoft SQL Server 2005 oder Microsoft SQL Server 2008 als Serverplattform für die Zieldatenbank.
  - **Eine neue Datenbank mit Datenbankobjekten erstellen:** Erstellt eine neue Microsoft SQL-Datenbank und füllt die neue Datenbank mit Datenbankobjekten aus
  - **Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen:** Fügt lediglich Datenbankobjekte zu einer bestehenden Microsoft SQL Server 2005-Datenbank hinzu. Die bestehende Datenbank muss leer sein.
  - Geben Sie das Verzeichnis für das Protokoll der Datenbankinstallation an.

  Klicken Sie anschließend auf "Weiter".
- Wenn Sie eine neue Datenbank erstellen, geben Sie die bestehenden Verzeichnisse an, die folgende Elemente aufnehmen sollen:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis
  - Protokollverzeichnis

  Klicken Sie anschließend auf "Weiter".
- Wenn Sie eine neue Datenbank erstellen, wählen Sie die gewünschte Option für die Zeichensatzunterstützung. Zur Auswahl stehen eine Unicode- oder eine reine ASCII-Datenbank. Wenn das Installationsprogramm in einer asiatischen Sprache ausgeführt wird, ist standardmäßig die Option für Unicode-Datenbanken festgelegt. Wenn das Installationsprogramm in einer nichtasiatischen Sprache ausgeführt wird, können Sie zwischen reinem ASCII-Format und Unicode wählen. Wählen Sie das gewünschte Datenbankformat aus und klicken Sie auf „OK“.

  Hinweis: Für die Unicode-Datenbankinstallation ist mehr Festplattenspeicher erforderlich als für die reine ASCII-Datenbankinstallation.

- Wenn Sie eine neue Datenbank erstellen, müssen Sie eine Option für die Datenbankgröße auswählen. Klicken Sie anschließend auf "Weiter".
- Wenn Sie eine neue Datenbank erstellen und als Datenbankgröße „Benutzerdefiniert“ ausgewählt haben, geben Sie die Einstellungen für die benutzerdefinierte Datenbankgröße an:
  - **Maximale Datenbankgröße:** Die maximale Menge an Festplattenspeicher, die die Datenbank belegen darf. Die Datenbank nimmt automatisch bis zu diesem Wert an Größe zu, während Daten darin angesammelt werden. Unabhängig von dem hier angegebenen Wert beträgt die Anfangsgröße der Datenbank 100 MB.

- **Protokolldateigröße:** Die Größe der Datei für das Transaktionsprotokoll.
- **Maximale Dateigröße für Datenbank:** Keine einzelne Datenbankdatei darf größer werden als dieser Wert.

Klicken Sie anschließend auf "Weiter".

Unter Linux/Solaris:

- Wählen Sie die Version des Oracle-Zieldatenbankservers sowie folgende Optionen aus:
  - **Eine neue Datenbank mit Datenbankobjekten erstellen:** Erstellt eine neue Oracle-Datenbankinstanz und füllt die neue Datenbank mit Datenbankobjekten aus
  - **Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen:** Fügt nur Datenbankobjekte zu einer bestehenden Oracle-Datenbankinstanz hinzu. Die bestehende Datenbank muss mit Ausnahme des Benutzers „esecdba“ leer sein.
  - Geben Sie das Verzeichnis für das Protokoll der Datenbankinstallation an.

  Klicken Sie anschließend auf "Weiter".
- Geben Sie den Oracle-Benutzernamen an oder akzeptieren Sie den Standardbenutzernamen. Klicken Sie auf "OK".
- Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Folgendes an:
  - **Der Pfad für die Oracle-JDBC-Treiberdatei:** Geben Sie den vollständigen Pfad zur jar-Datei an, für gewöhnlich `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (Umgebungsvariablen können in diesem Feld jedoch nicht verwendet werden).
  - **Hostname:** Der Hostname des lokalen Computers, auf dem die Oracle-Datenbank installiert ist. Das Installationprogramm unterstützt die Erstellung einer neuen Datenbankinstanz nur auf dem lokalen Host.
  - **Datenbankname:** Der Name der zu erstellenden Datenbankinstanz.
- Wenn Sie einer vorhandenen leeren Oracle-Datenbank Datenbankobjekte hinzufügen, werden Sie um die folgenden Informationen gebeten.
  - **Der Pfad für die Oracle-JDBC-Treiberdatei:** Geben Sie den vollständigen Pfad zur jar-Datei an, für gewöhnlich `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (Umgebungsvariablen können in diesem Feld jedoch nicht verwendet werden).
  - **Datenbank-Hostname oder IP-Adresse:** Der Hostname bzw. die IP-Adresse des Computers, auf dem die Oracle-Datenbank installiert ist. Das kann der lokale Hostname oder ein Remote-Hostname sein.
  - **Datenbankname:** Der Name der bestehenden leeren Oracle-Datenbankinstanz (Standard: „ESEC“). Dieser Datenbankname muss als Servicename in der Datei `tnsnames.ora` (im Verzeichnis $ORACLE_HOME/network/admin/) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, angezeigt werden.
  - **Datenbankport:** Der Standardwert ist „1521“
  - **Passwort:** Geben Sie für Sentinel-Datenbankadministratoren (DBA) das Passwort für den Benutzer „esecdba“ ein. Das Benutzernamenfeld in dieser Eingabeaufforderung lässt sich nicht bearbeiten.

Hinweis: Wenn der Datenbankname nicht in der Datei `tnsnames.ora` enthalten ist, gibt das Installationsprogramm zu diesem Zeitpunkt in der Installation keinen Fehler aus (weil es die Verbindung über eine direkte JDBC-Verbindung überprüft). Die Datenbankinstallation scheitert erst dann, wenn das Datenbankinstallationsprogramm

versucht, die Verbindung mit der Datenbank über „sqlplus“ herzustellen. Wenn die Datenbankinstallation zu diesem Zeitpunkt scheitert, sollten Sie – ohne das Installationsprogramm zu beenden – den Service-Namen für die Datenbank in der Datei `tnsnames.ora` auf dem betreffenden Computer ändern, im Installationsprogramm zum ersten Bildschirm zurückblättern und dann den Vorgang erneut durchführen. Dadurch wird versucht, die Datenbankinstallation mit den neuen Werten in der Datei `tnsnames.ora` durchzuführen.

Hinweis: Das Installationsprogramm sichert alle bestehenden `tnsnames.ora`- und `listener.ora`-Dateien im Verzeichnis „$ORACLE_HOME/network/admin“. Die Datei `listener.ora` wird mit Verbindungsinformationen für die Sentinel-Datenbank überschrieben und die Datei `tnsnames.ora` wird mit Verbindungsinformationen für die Sentinel-Datenbank ergänzt. Wenn sich weitere Datenbanken auf demselben Server wie die Sentinel-Datenbank befinden, muss der Administrator manuell Informationen aus den gesicherten `listener.ora`-Dateien in der neuen Datei zusammenführen und den Oracle-Listener neu starten, damit andere Anwendungen weiterhin eine Verbindung mit der Datenbank herstellen können.

- Wenn Sie eine neue Datenbankinstanz erstellen, müssen Sie die Arbeitsspeicher-(RAM-)Zuweisung für Oracle und den Listener-Port angeben oder die Standardwerte akzeptieren.
- Wenn Sie eine neue Datenbankinstanz erstellen, geben Sie die Passwörter an, die für die standardmäßigen SYS- und SYSTEM-Datenbankbenutzer gelten sollen. Klicken Sie anschließend auf "Weiter".
- Wenn Sie eine neue Datenbankinstanz erstellen, müssen Sie eine Option für die Datenbankgröße auswählen. Klicken Sie anschließend auf "Weiter".
- Wenn Sie eine neue Datenbankinstanz erstellen und als Datenbankgröße „Benutzerdefiniert“ ausgewählt haben, geben Sie die Einstellungen für die benutzerdefinierte Datenbankgröße an:
  - **Maximale Datenbankgröße:** Die maximale Menge an Festplattenspeicher, die die Datenbank belegen darf. Die Datenbank nimmt automatisch bis zu diesem Wert an Größe zu, während Daten darin angesammelt werden. Unabhängig von dem hier angegebenen Wert beträgt die Anfangsgröße der Datenbank 5000 MB.
  - **Protokolldateigröße:** Die Größe der einzelnen Wiederherstellungsprotokolldateien
  - **Maximale Dateigröße für Datenbank:** Keine einzelne Datenbankdatei darf größer werden als dieser Wert.
- Wenn Sie eine neue Datenbankinstanz erstellen, geben Sie die bestehenden Verzeichnisse an, die als Datenbankspeicher verwendet werden sollen:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis
  - Temporäres Verzeichnis und Verzeichnis zum Rückgängigmachen
  - Verzeichnis für Redo-Protokollmitglied A
  - B-Verzeichnis für Protokollmitglied neu erstellen

  Klicken Sie anschließend auf "Weiter".

Hinweis: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung empfiehlt Novell, dass diese Speicherorte auf unterschiedlichen E/A-Geräten liegen sollten.

Zugunsten einer möglich effizienten Funktionsweise sollte das Wiederherstellungsprotokoll auf den schnellsten Schreibdatenträger verweisen, der Ihnen zur Verfügung steht.

Das Installationsprogramm erstellt diese Verzeichnisse nicht. Sie müssen daher extern erstellt werden, bevor über diesen Schritt hinausgegangen wird, und der Oracle-Benutzer muss über Schreibrechte für diese Verzeichnisse verfügen. Weitere Informationen finden Sie unter Abschnitt 3.3.2, „Voraussetzungen für die Sentinel-Datenbankinstallation“, auf Seite 35.

18 Wenn Sie ausgewählt haben, dass die Datenbankkomponente installiert werden soll, müssen Sie die Datenbankpartitionen konfigurieren.

- Wählen Sie die Option „Automatische Datenbankpartitionen aktivieren“, um Sentinel Data Manager die Verwaltung der Datenbankpartitionierung und -archivierung zu gestatten.
- Geben Sie bei Datenpartitionen ein bestehendes Verzeichnis für Archivdateien an.
- Geben Sie die Startzeit für das Hinzufügen von Partitionen und die Archivierung von Daten an. Diese Vorgänge sollten sich nicht überlappen, da sie dieselben Ressourcen verwenden.

Klicken Sie anschließend auf "Weiter".

19 Wenn Sie sich für die Installation der Datenbankkomponente entschieden haben, müssen Sie Authentifizierungsinformationen für folgende Elemente angeben:

- Sentinel-Datenbank-Administrationsbenutzer
- Sentinel-Anwendungsdatenbankbenutzer
- Sentinel-Administratorbenutzer
- Sentinel Report-Benutzer (nur unter Windows)

Hinweis: Wenn auch die DAS-Komponente installiert wird, ist das Benutzerpasswort für die Sentinel-Anwendungsdatenbank auch dann erforderlich, wenn die Windows-Authentifizierung gewählt wird. Dies ist erforderlich, um den Sentinel-Service für die Anmeldung als Sentinel-Anwendungsdatenbankbenutzer zu installieren. Alle anderen Benutzer müssen kein Passwort angeben, wenn sie die Windows-Authentifizierung verwenden.

Klicken Sie anschließend auf "Weiter".

20 Wenn Sie sich für die Installation der Datenbankkomponente entschieden haben, wird eine Übersicht über die angegebenen Datenbankparameter angezeigt. Klicken Sie anschließend auf "Weiter".

21 Wenn Sie sich für die Installation einer oder mehrerer Sentinel Server-Komponenten entschieden haben, werden Sie aufgefordert, die Menge an Arbeitsspeicher (RAM) anzugeben, die diesen Komponenten zugeordnet werden soll. Das Installationsprogramm berücksichtigt

den Betriebssystem- und Datenbank-Overhead bei der Bestimmung der anzuzeigenden Zuordnungsoptionen. Es gibt zwei Möglichkeiten für die Angabe der Arbeitsspeicherzuordnung:

- **Automatische Konfiguration des Arbeitsspeichers:** Wählen Sie aus, wie viel Arbeitsspeicher Sentinel Server insgesamt zugewiesen werden soll. Das Installationsprogramm bestimmt automatisch die optimale Verteilung des Arbeitsspeichers unter den Komponenten und berücksichtigt dabei den geschätzten Betriebssystem- und Datenbank-Overhead.

  Wichtig: Sie können den -Xmx-Wert in der Datei `configuration.xml` bearbeiten, um die RAM-Zuordnung für die Sentinel Server-Prozesse zu ändern. Die Datei `configuration.xml` wird bei Linux/Solaris unter `$ESEC_HOME/config` und bei Windows unter `%ESEC_HOME%\config` abgelegt.

- **Benutzerdefinierte Konfiguration des Arbeitsspeichers** Klicken Sie auf die Schaltfläche „Konfigurieren...“, um eine Feinabstimmung der Arbeitsspeicherzuordnung vorzunehmen. Diese Option ist nur verfügbar, wenn genügend Arbeitsspeicher auf dem Computer vorhanden ist.

22 Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, wird folgende Eingabeaufforderung angezeigt, in der Sie nach dem Aktualisierungstyp gefragt werden:

- **Direktes Herunterladen vom Internet:** In dieser Konfiguration werden regelmäßig automatisch Aktualisierungen von Novell über das Internet heruntergeladen (alle 6 oder 12 Stunden). Verwenden Sie diese Option, wenn der Computer über einen direkten Zugang zum Internet verfügt.
- **Einzelplatzbetrieb:** In dieser Konfiguration müssen für die Aktualisierung von Advisor Dateien manuell von Novell heruntergeladen werden. Verwenden Sie diese Option, wenn der Computer nicht über einen direkten Zugang zum Internet verfügt.

23 Wenn Sie sich für die Installation von Advisor entschieden und festgelegt haben, dass das direkte Herunterladen vom Internet verwendet werden soll, müssen Sie den Novell eLogin-Namen und das Passwort für die Advisor-Lizenz angeben und festlegen, wie oft die Advisor-Daten aktualisiert werden sollen (alle 6 oder 12 Stunden). Klicken Sie anschließend auf "Weiter".

24 Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, geben Sie Folgendes an:

- Die Senderadresse („Von“), die in Advisor-bezogenen Email-Benachrichtigungen angezeigt werden soll
- Die Empfängeradresse („An“) für Advisor-bezogene Email-Benachrichtigungen

  Hinweis: Nach der Installation können Sie die Advisor-Email-Adressen durch Bearbeiten des Abschnitts „AdvisorService“ der Datei `advisor_client.xml` im Verzeichnis „$ESEC_HOME/config“ ändern. Weitere Informationen finden Sie unter “Registerkarte „Advisor““ im *Sentinel-Benutzerhandbuch*.

- Wählen Sie aus, ob Sie per Email über erfolgreiche Advisor-Aktualisierungen benachrichtigt werden möchten.

  Hinweis: Fehlermeldungen werden unabhängig von der gewählten Option immer versendet.

Hinweis: Wenn Sie sich für die Installation von HP Service Desk entschieden haben, werden Sie zur Eingabe weiterer Informationen aufgefordert.

25 Klicken Sie anschließend auf "Weiter". Ein Übersichtsbildschirm mit den für die Installation ausgewählten Funktionen wird angezeigt. Klicken Sie auf Installieren.

26 Wenn der Collector Manager für die Installation ausgewählt und für die Verwendung der Proxy-Kommunikation konfiguriert wurde, werden Sie zur Eingabe von Benutzernamen und Passwort eines Sentinel-Benutzers aufgefordert, der über die Berechtigung zur Registrierung eines verbürgten Clients verfügt (Beispiel: „esecadm“). Um diesen Schritt abzuschließen, muss der Communication Server ausgeführt werden, und ein gültiger Benutzername und ein gültiges Passwort müssen angegeben werden. Zur Registrierung eines verbürgten Client gehört die Annahme des SSL-Zertifikats des Communication Server und das Hochladen des SSL-Zertifikats des Collector Managers auf den Communication Server. Wenn die Verbindung mit dem Communication Server initiiert wird, werden Sie aufgefordert, das Zertifikat des Servers zu akzeptieren. Überprüfen Sie die Attribute des Zertifikats und wählen Sie dann die Option „Dauerhaft akzeptieren“. Das Installationsprogramm lädt dann automatisch das Zertifikat des Collector -Manager auf den Communication Server hoch.

27 Nach der Installation werden Sie aufgefordert, neu zu booten oder sich erneut anzumelden und Sentinel Services manuell zu starten. Klicken Sie auf „Fertig stellen“, um das System neu zu booten. (Geplante Services wie das Herunterladen von Advisor können erst nach dem erneuten Booten ausgeführt werden.)

Hinweis: Das Sentinel-Installationsprogramm deaktiviert standardmäßig die Archivprotokollierung. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank möglicherweise keine Ereignisse mehr entgegen.

3.6.1 Konsoleninstallation unter Linux/Solaris

Bei Verwendung des „Konsolen“-Modus werden auf der Komponentenauswahlseite des Installationsprogramms nicht alle Komponenten zusammen angezeigt. Befolgen Sie die Bildschirmanweisungen zur Anzeige und Bearbeitung der ausgewählten untergeordneten Komponenten.

Im Folgenden sehen Sie ein Beispiel für die Navigation auf der Komponentenauswahlseite des Konsolen-Modus:

```
Sentinel 6.1 - InstallShield Wizard
Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 1
```

```
Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [x] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
    Enter command [1] 2

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services

      To select/deselect a feature or to view its children, type its
number:
        1.  [ ] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1.  [x] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 2

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1.  [x] Communication Server
        2.  [x] Advisor (Requires Advisor ID and Password)
```

```
 3.  [x] Correlation Engine
 4.  [x] Data Access Server
 5.  [x] Sentinel Collector Service
Other options:
 -1. View this feature's parent
 0. Continue installing
```

3.7 Installation von Sentinel als Domänenbenutzer

So installieren Sie Sentinel als Domänenbenutzer:

1. Ordnen Sie jedem der Sentinel-Benutzer einen Domänenbenutzer zu (esecdba, esecadm, esecrpt).
2. Führen Sie die in Abschnitt 3.3.1, „Erteilen von Hauptbenutzer-Privilegien für „Domänenbenutzer““, auf Seite 35 angegebenen Aktionen aus, um Hauptbenutzerberechtigungen anzugeben.
3. Installieren Sie Sentinel 6.0 als Administratorbenutzer. Informationen zur Installation von Sentinel finden Sie inAbschnitt 3.6, „Benutzerdefinierte Installation“, auf Seite 46.
4. Wenn das Installationsprogramm Sie zur Eingabe des Berechtigungsnachweises für die Benutzer „esecdba“, „esecadm“ und „esecrpt“ auffordert, geben Sie den erstellten Domänenbenutzer im Format „Domäne\Domänenbenutzer“ an, geben Sie das Passwort ein und fahren Sie mit der Installation fort.

3.8 Konfiguration nach der Installation

3.8.1 Konfigurieren des SMTP-Integrators für das Senden von Sentinel-Benachrichtigungen

In Sentinel 6.1 arbeitet eine JavaScript `SendEmail`-Aktion mit einem SMTP-Integrator zusammen, um Emails aus verschiedenen Kontexten innerhalb der Sentinel-Schnittstelle an die Email-Empfänger zu senden. Die Empfänger der Email und des Nachrichteninhalts werden in den Aktionsparametern konfiguriert.

In jeder Sentinel-Installation wird automatisch eine Aktionsinstanz des Aktions-Plugins `SendEmail` erstellt. Diese Aktion wird intern von Sentinel verwendet, um Emails in den folgenden Situationen zu senden:

- Wenn eine Korrelationsregel ausgelöst wird, die mit einer Aktion „Email senden“ bereitgestellt wird. Die hier erwähnte Aktion „Email senden“ ist die vom Zahnradsymbol angegebene Aktion, die nur für die Korrelation gültig ist (im Gegensatz zur JavaScript-Aktion `SendEmail` , die vom JS JavaScript angegeben wird).
- Zum Workflow gehört ein Emailschritt oder eine Aktivität, die zum Senden von Email konfiguriert ist.
- Der Benutzer öffnet einen Vorfall und führt eine Aktivität aus, die zum Senden von Email konfiguriert ist.

- Der Benutzer klickt mit der rechten Maustaste auf ein Ereignis und wählt „Email“.
- Der Benutzer öffnet einen Vorfall und wählt „Vorfall mailen“.
- Der Advisor-Download sendet eine Benachrichtigung.

Die Aktion `SendEmail` muss nicht konfiguriert werden. Der SMTP Integrator muss jedoch mit gültigen Verbindungsinformationen konfiguriert sein.

3.8.2 Sentinel-Datenbank

Verwendet der Datenbankadministrator keine eigenen Prozeduren, aktivieren Sie die automatische Partitionsverwaltung der Sentinel-Datenbank (Archivieren, Ablegen und Hinzufügen von Partitionen) bei der Installation. Dadurch halten Sie die Menge der Ereignisdaten im Rahmen. Automatische Partitionsverwaltung kann mithilfe von Sentinel Data Manager (SDM) auch nach der Installation konfiguriert werden.

Standardmäßig kann der Sentinel Data Manager unter Umständen zum Archivieren von Daten nicht in das Dateisystem schreiben. Sie können dies durch Bearbeiten der Datei „init<OracleSID>.ora“ für die Datenbank aktivieren.

Hinweis: Standardmäßig legt das Installationsprogramm für alle Tabellenbereiche ein automatisches Wachstum fest. Standardmäßig liegt die Obergrenze für das Dateiwachstum bei 200 MB, die maximale Dateigröße hängt jedoch von dem während der Installation angegebenen Wert ab.

So aktivieren Sie die Schreibfunktion in das Archivverzeichnis durch Oracle:

1. Melden Sie sich beim Datenbankcomputer an:
2. Wechseln Sie in das Verzeichnis „$ORACLE_HOME/dbs“.
3. Öffnen Sie die Datei init`<OracleSID>.ora` in einem Texteditor.
4. Bearbeiten Sie den Parameter „UTL_FILE_DIR“, um den Verzeichnispfad anzugeben, in den die archivierten Sentinel-Daten geschrieben werden sollen. Folgendes muss angegeben werden:
   - UTL_FILE_DIR = *

     oder
   - UTL_FILE_DIR = [spezieller Verzeichnispfad]
5. Speichern Sie die Datei und beenden Sie den Vorgang.

3.8.3 Collector-Service

Während der Installation des Collector Service wird ein Collector (Sammelstelle) mit dem Namen „Allgemeiner Collector“ konfiguriert. Standardmäßig erstellt er 5 Ereignisse pro Sekunde (eps). Dieser Collector kann zum Testen der Installation verwendet werden. Weitere Collectors können auf der Novell-Website (http://support.novell.com/products/sentinel/collectors.html) heruntergeladen werden.

3.8.4 Aktualisieren des Lizenzschlüssels (vom Evaluations- zum Produktionsschlüssel)

Wenn Sie dieses Produkt nach der Evaluation erwerben, sollten Sie den Lizenzschlüssel im System mit dem unten angegebenen Verfahren aktualisieren, damit keine erneute Installation erforderlich ist.

So aktualisieren Sie Ihren Lizenzschlüssel (UNIX):

1. Melden Sie sich an dem Computer, auf dem die DAS-Komponente installiert ist, als Sentinel-Administrator-Betriebssystembenutzer an (Standard: „esecadm“).
2. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis „$ESEC_HOME/bin“
3. Geben Sie folgenden Befehl ein:

   ```
   ./softwarekey.sh
   ```
4. Geben Sie die Zahl 1 ein, um Ihren Primärschlüssel festzulegen. Drücken Sie die EINGABETASTE.

So aktualisieren Sie Ihren Lizenzschlüssel (Windows):

1. Melden Sie sich an dem Computer, auf dem die DAS-Komponente installiert ist, als Benutzer mit Administratorrechten an.
2. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis „%ESEC_HOME%\bin“.
3. Geben Sie folgenden Befehl ein:

   ```
   .\softwarekey.bat
   ```
4. Geben Sie die Zahl 1 ein, um Ihren Primärschlüssel festzulegen. Drücken Sie die EINGABETASTE.

3.8.5 Starten des Collector Manager Service

So starten Sie den Collector Manager Service

1. Starten Sie Sentinel 6.1
2. Klicken Sie auf die Registerkarte „Admin“ > „Ansicht der Server“. Alternativ können Sie auch im Fensterbereich „Navigator“ auf „Ansicht der Server“ klicken.
3. Erweitern Sie die Ansicht „Server“. Die Liste der Prozesse wird angezeigt.

   Klicken Sie mit der rechten Maustaste auf den zu startenden Collector Manager; wählen Sie „Aktionen“ > „Starten“.

Oder

1. Starten Sie Sentinel 6.1
2. Klicken Sie auf „Ereignisquellenverwaltung“ > „Live-Ansicht“
3. Klicken Sie mit der rechten Maustaste im Fenster “Ereignisquellenverwaltung (Live-Ansicht)“ auf den zu startenden Collector Manager; wählen Sie „Starten“.

3.8.6 Zeitverwaltung

Novell empfiehlt dringend, alle Sentinel-Komponenten, insbesondere die Computer für Correlation Engine und Collector Manager, mit einem NTP-(Network Time Protocol-)Server oder einem anderen Zeitservertyp zu verbinden. Wenn die Systemzeit nicht zwischen den einzelnen Computern synchronisiert ist, funktionieren Sentinel Correlation Engine und Active Views nicht ordnungsgemäß. Die Ereignisse von den Collector Managers werden nicht als Echtzeitereignisse betrachtet und daher unter Umgehung der Sentinel Control Center und Correlation Engines direkt an die Sentinel-Datenbank gesendet.

Standardmäßig liegt der Schwellenwert für „Echtzeit“-Daten bei 120 Sekunden. Diese Vorgabe kann durch eine Änderung des Werts `esecurity.router.event.realtime.expiration` in der Datei `event-router.properties` geändert werden. Die Sentinel-Ereignisuhrzeit wird entsprechend der Uhrzeit des Trust Device oder des Collector Managers ausgefüllt. Die Uhrzeit des Trust Device kann während der Konfiguration eines Collector ausgewählt werden. Die Uhrzeit des Trust Device ist der Zeitpunkt, an dem das Protokoll vom Gerät erstellt wurde. Die Collector Manager-Uhrzeit ist die lokale Systemzeit des Collector Manager-Systems.

3.8.7 Bearbeiten der Oracle-Skripts „dbstart“ und „dbshut“

Sentinel kann die Oracle 10-Datenbank aufgrund von Fehlern in den Oracle-Skripts `dbstart` und `dbshut` nicht starten. Details zu den Skriptfehlern finden Sie unter https://metalink.oracle.com (https://metalink.oracle.com) für die Fehlernummer 336299.1 mit dem Betreff „dbstart errors out when executing in 10.2.0.1.0“ und die Fehlernummern 5183726 und 4665320.

Nach der Installation von Sentinel 6 müssen Sie die Skripts `dbstart` und `dbshut` für Sentinel bearbeiten, um eine Oracle 10-Datenbank starten zu können.

So bearbeiten Sie das Skript „dbstart“ unter Solaris 10:

1. Öffnen Sie das Skript `dbstart` im Pfad „$ORACLE_HOME/bin/dbstart“ zur Bearbeitung.
2. Gehen Sie zu Zeile 78 und ersetzen Sie sie durch „ORACLE_HOME_LISTNER=$ORACLE_HOME“.
3. Fügen Sie `#!/bin/bash` am Anfang hinzu, um die bash-Shell anzufordern.
4. Vergewissern Sie sich, dass „ORATAB“ auf „ORATAB=/var/opt/oracle/oratab“ verweist.

   Hinweis: Wenn sich ORATAB nicht an dem oben angegebenen Standort auf Ihrem Computer befindet, ändern Sie den ORATAB-Pfad manuell auf den genauen Standort.
5. Klicken Sie auf „Speichern“ und verlassen Sie das Skript.
6. So bearbeiten Sie das Skript „dbshut“ unter Solaris 10:
7. Öffnen Sie das Skript „dbshut“ im Pfad$ORACLE_HOME/bin/dbshut zur Bearbeitung.
8. Vergewissern Sie sich, dass „ORATAB“ auf „ORATAB=/var/opt/oracle/oratab“ verweist.

   Hinweis: Wenn sich ORATAB nicht an dem oben angegebenen Standort auf Ihrem Computer befindet, ändern Sie den ORATAB-Pfad manuell auf den genauen Standort.
9. Klicken Sie auf „Speichern“ und verlassen Sie das Skript.

So bearbeiten Sie das Skript „dbstart“ unter RedHat Linux ES4:

1. Öffnen Sie das Skript `dbstart` im Pfad „$ORACLE_HOME/bin/dbstart“ zur Bearbeitung.
2. Vergewissern Sie sich, dass „ORATAB“ auf „ORATAB=/etc/oratab“ verweist.

   Hinweis: Wenn sich ORATAB nicht an dem oben angegebenen Standort auf Ihrem Computer befindet, ändern Sie den ORATAB-Pfad manuell auf den genauen Standort.
3. Klicken Sie auf „Speichern“ und verlassen Sie das Skript.
4. So bearbeiten Sie das Skript „dbshutt“ unter RedHat Linux ES4:
5. Öffnen Sie das Skript `dbshut` im Pfad$ORACLE_HOME/bin/dbstart zur Bearbeitung.
6. Vergewissern Sie sich, dass „ORATAB“ auf „ORATAB=/etc/oratab“ verweist.

   Hinweis: Wenn sich ORATAB nicht an dem oben angegebenen Standort auf Ihrem Computer befindet, ändern Sie den ORATAB-Pfad manuell auf den genauen Standort.
7. Klicken Sie auf „Speichern“ und verlassen Sie das Skript.

Advisor-Konfiguration

4

- Abschnitt 4.1, „Advisor-Überblick“, auf Seite 65
- Abschnitt 4.2, „Informationen zur Installation von Advisor“, auf Seite 66
- Abschnitt 4.3, „Installation von Advisor“, auf Seite 68
- Abschnitt 4.4, „Advisor-Berichte“, auf Seite 74
- Abschnitt 4.5, „Wartung von Advisor“, auf Seite 75

In diesem Abschnitt werden das Laden von Advisor-Daten, die Konfiguration regelmäßiger Aktualisierungen zu den Advisor-Daten und die Konfiguration von Sentinel für die Ausführung von Advisor Reports (von Novell bereitgestellt) über die Registerkarte „Advisor“ des Sentinel Control Center behandelt.

4.1 Advisor-Überblick

Advisor ist ein optionaler Abonnement-Service, der eine Korrelation auf Geräteebene zwischen Echtzeitereignissen aus Intrusion Detection- und Prevention-Systemen und den Ergebnissen von unternehmensweiten Vulnerability-Scans herstellt. Durch die Bereitstellung normalisierter Angriffsinformationen fungiert Advisor als Frühwarnsystem für die Erkennung von Angriffen gegen anfällige Systeme („Schwachstellenerkennung“). Außerdem stellt es die entsprechenden Informationen zur Abhilfe bereit.

Hinweis: Die Installation von Advisor ist optional. Die Komponente ist allerdings notwendig, wenn Sie die Sentinel-Funktion zur Schwachstellenerkennung oder die Advisor-Berichtsfunktion nutzen möchten. Advisor ist ein abonnementbasierter Datenservice, für den eine zusätzliche Lizenz von Novell erforderlich ist.

Die unterstützten Systeme werden unten mit dem zugehörigen Gerätetyp („IDS“ für „Intrusion Detection-System“, „VULN“ für „Vulnerability-Scanner“, und „FW“ für „Firewall“) aufgelistet.

Tabelle 4-1 *Unterstützte Systeme und zugehörige Gerätetypen*

Unterstützte Systeme	Gerätetyp	RV31-Wert
Cisco Secure IDS	IDS	Secure
Enterasys Dragon Host Sensor	IDS	Dragon
Enterasys Dragon Network Sensor	IDS	Dragon Network
Intrusion.com (SecureNet_Provider)	IDS	SecureNet_Provider
ISS BlackICE PC Protection	IDS	BlackICE
ISS RealSecure Desktop	IDS	RealSecure Desktop
ISS RealSecure Network	IDS	RealSecure

Unterstützte Systeme	Gerätetyp	RV31-Wert
ISS RealSecure Server	IDS	RealSecure Server
ISS RealSecure Guard	IDS	RealSecure Guard
Sourcefire Snort/Phalanx	IDS	Snort
Symantec Network Security 4.0 (ManHunt)	IDS	ManHunt
Symantec Intruder Alert	IDS	Intruder
McAfee IntruShield	IDS	IntruShield
eEYE Retina	VULN	Retina
Foundstone Foundscan	VULN	Foundstone
ISS Database Scanner	VULN	Database Scanner
ISS Internet Scanner	VULN	Internet Scanner
ISS System Scanner	VULN	System Scanner
ISS Wireless Scanner	VULN	Wireless Scanner
Nessus	VULN	Nessus
nCircle IP360	VULN	nCircle IP360
Qualys QualysGuard	VULN	QualysGuard
Cisco IOS Firewall	FW	Cisco IOS

Um die Schwachstellenerkennung vollständig aktivieren zu können, müssen die Sentinel-Collectors mehrere Variablen korrekt ausfüllen. Von Novell erstellte Collectors (Sammelstellen) füllen diese Variablen standardmäßig aus.

- Im IDS Collector muss RV39 (MSSPCustomerName) auf den „MSSP Customer Name“ gesetzt sein.
- Bei IDS- und Vulnerability-Collectors muss die Variable RV31 („reserved value“ – „reservierter Wert“) auf den Wert gesetzt werden, der oben in der Tabelle in der Spalte „RV31“ steht. Bei dieser Zeichenkette muss die Groß-/Kleinschreibung beachtet werden.
- Beim IDS-Collector muss die DIP („Destination IP“ – „Ziel-IP“) mit der IP-Adresse des Computers ausgefüllt werden, der angegriffen wird.
- Beim IDS-Collector muss die RT1 (DeviceAttackName) auf den Angriffsnamen oder Angriffscode des betreffenden IDS gesetzt werden.

Von Novell erstellte Collectors (Sammelstellen) legen diese Variablen standardmäßig fest.

4.2 Informationen zur Installation von Advisor

Die beiden Hauptkomponenten einer Advisor-Installation bestehen in der Konfiguration der regelmäßigen Updates, die im Datenabonnement-Service enthalten sind, und dem Laden des Anfangssatzes an Advisor-Daten.

Beim Laden der Anfangsdaten empfiehlt Novell dringend die Verwendung des Advisor Core Data ISO, das über das Novell-Kundenserviceportal für Kunden zur Verfügung steht, die das Advisor-Datenabonnement erworben haben. Dieses Installationsprogramm lädt ca. 10 GB an Daten, die ansonsten mithilfe des regelmäßigen Aktualisierungsservice über das Netzwerk übertragen werden müssten.

Standardmäßig sind die Skripts, die automatische Downloads initiieren, deaktiviert. Aktivieren Sie die Skripts, nachdem die Advisor Core-Daten geladen wurden.

Advisor muss auf demselben Computer installiert wie der Database Access Service (DAS) werden. Die regelmäßigen Aktualisierungen können manuell oder automatisch sein. Dies hängt von Ihrer Auswahl im Sentinel-Installationsprogramm ab.

- **Einzelplatzbetrieb:** Manuelle Aktualisierungen
- **Direktes Herunterladen vom Internet:** geplant, automatische Aktualisierungen

---

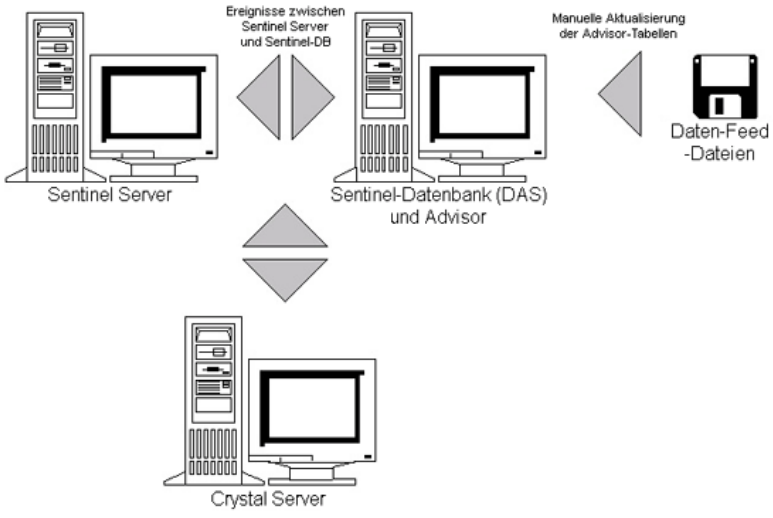
Hinweis: Der Advisor-Datenfeed für Sentinel 6.0 SP2 und höher wurde durch zusätzliche Signaturen erweitert. Die Änderungen in SP2 betreffen sowohl den erforderlichen Speicherplatz als auch die Installationsprozeduren.

Novell empfiehlt ca 50 GB Festplattenspeicher für die Advisor-Daten, zusätzlich zu dem erforderlichen Speicherplatz für die Sentinel-Daten selbst.

4.2.1 Einzelplatzkonfiguration

Eine Einzelplatzinstallation ist eine Installation, bei der Advisor ein isoliertes System ist, bei dem manuelle Aktualisierungen an den Advisor-Daten erforderlich sind. Advisor-Installationen in einer sicheren Umgebung besitzen häufig keine Internetverbindungen und müssen daher als Einzelplatzkonfigurationen erfolgen.

Abbildung 4-1 *Einzelplatzkonfiguration*



Bei der Einzelplatzkonfiguration können die Advisor-Daten manuell von einem der folgenden Standorte heruntergeladen werden:

- Sentinel 6.0 SP1 und niedriger:

  https://advisor.novell.com/advisordata/ (https://advisor.novell.com/advisordata/)

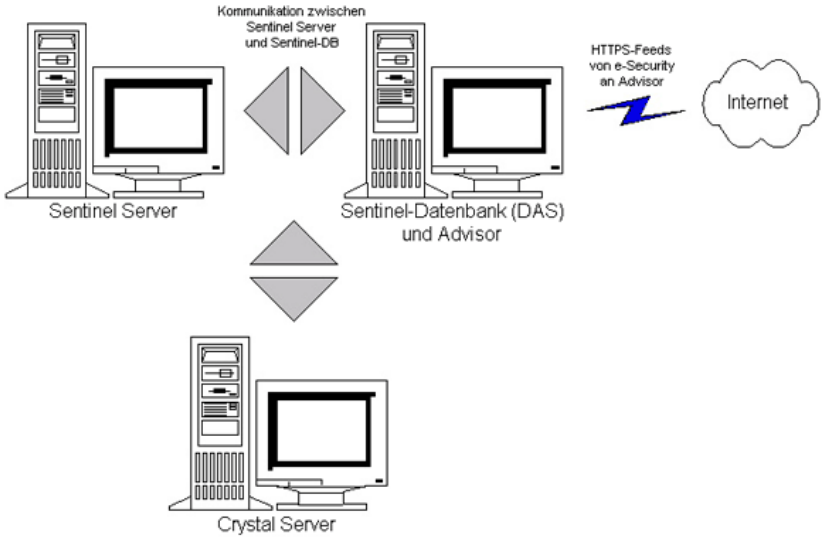
- Sentinel 6.0 SP2 und höher:

  https://secure-www.novell.com/sentinel/advisor/advisordata (https://secure-www.novell.com/sentinel/advisor/advisordata)

4.2.2 Konfiguration für direktes Herunterladen vom Internet

Beim direkten Herunterladen vom Internet ist der Advisor-Computer direkt mit dem Internet verbunden. Bei dieser Konfiguration werden die Advisor-Daten regelmäßig (alle 6 oder 12 Stunden) automatisch über das Internet von Novell heruntergeladen. Weitere Informationen finden Sie unterKapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31.

Abbildung 4-2 *Direktes Herunterladen vom Internet*



4.3 Installation von Advisor

Advisor kann im Rahmen der Sentinel-Installation oder als zusätzliche Komponente installiert werden.

Hinweis: Die Advisor-Konfiguration hat sich zwischen Sentinel 6.0 SP1 und 6.0 SP2 maßgeblich geändert. Wenn Sie 6.0 SP1 oder niedriger verwenden, lesen Sie in der entsprechenden Version der Dokumentation unter http://www.novell.com/documentation/sentinel6 (http://www.novell.com/documentation/sentinel6.) nach.

So installieren Sie Advisor:

1 Melden Sie sich unter Solaris/Linux als Benutzer „root“ bzw. unter Windows als Administratorbenutzer an.

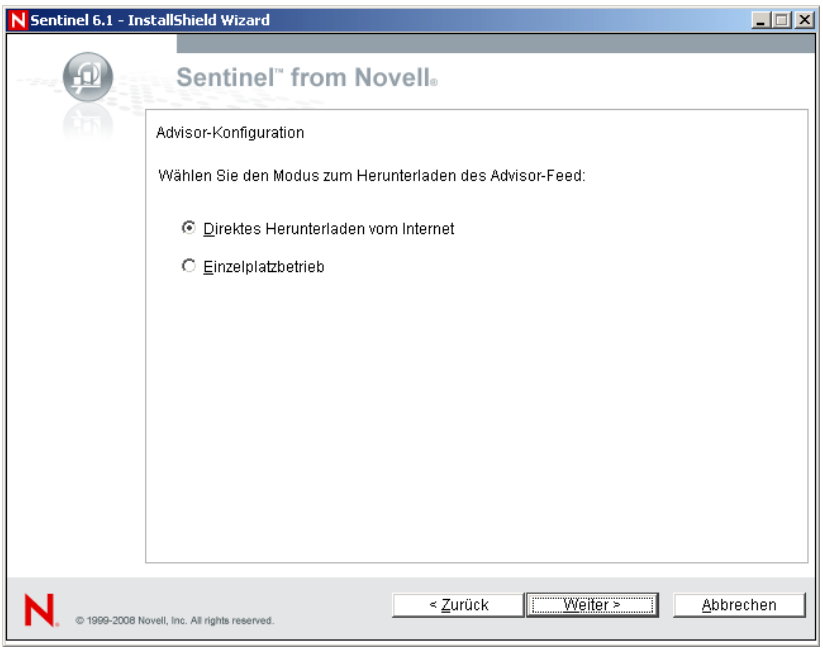
2. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
3. Starten Sie das Installationsprogramm. Wechseln Sie dazu in das Installationsverzeichnis auf der CD-ROM und gehen Sie dann wie folgt vor:
   - Unter Windows: Führen Sie `setup.bat` aus.
   - Unter Solaris/Linux:

     Für GUI-Modus:

     ```
     ./setup.sh
     ```

     Oder für den textbasierten Modus („serielle Konsole“):

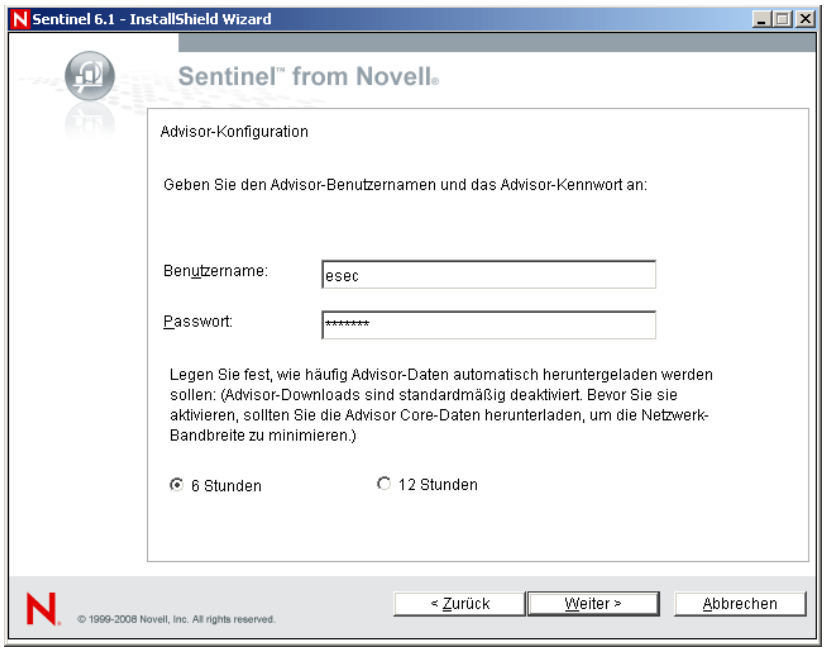
     ```
     ./setup.sh -console
     ```
4. Wählen Sie die entsprechende Sprache aus und klicken Sie auf „OK“.
5. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.
6. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie dann auf „Weiter“.
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie anschließend auf "Weiter".
8. Wählen Sie „Benutzerdefiniert“ aus. Klicken Sie anschließend auf "Weiter".
9. Geben Sie in diesem Fenster die Konfigurationsinformationen an und klicken Sie auf „Weiter“.
   - Seriennummer
   - Lizenzschlüssel
   - Globales Systempasswort
   - Das hier eingegebene Passwort gilt für alle Standardbenutzer. Dazu gehören sowohl der Sentinel-Administratorbenutzer als auch die Datenbankbenutzer. Weitere Informationen zur Liste der mithilfe der Installation erstellten Standarddatenbankbenutzer finden Sie inAbschnitt 3.8.2, „Sentinel-Datenbank“, auf Seite 60.
10. Wählen Sie eine der beiden verfügbaren Optionen: „Direktes Herunterladen vom Internet“ oder „Einzelplatzbetrieb“



11 Wenn Sie „Direktes Herunterladen vom Internet“ ausgewählt haben, geben Sie folgende Informationen an:

- Advisor-Benutzername
- Advisor-Passwort
- Aktualisierungshäufigkeit für die Advisor-Daten

Hinweis: Bei Sentinel 6.0 SP2 und höher handelt es sich beim Advisor-Benutzernamen und dem zugehörigen Passwort um die Novell eLogin-Daten, die zu dem Sentinel-Kauf gehören. Diese Anmeldedaten können, müssen jedoch nicht den Novell eLogin-Daten, die zum Sentinel-Kauf gehören, entsprechen. Weitere Informationen finden Sie im Abschnitt “Registerkarte „Advisor“” im *Sentinel-Benutzerhandbuch*.


Sentinel 6.1 - InstallShield Wizard
Sentinel™ from Novell®
Advisor-Konfiguration
Geben Sie den Advisor-Benutzernamen und das Advisor-Kennwort an:
Benutzername:
esec
Passwort:
****
Legen Sie fest, wie häufig Advisor-Daten automatisch heruntergeladen werden sollen: (Advisor-Downloads sind standardmäßig deaktiviert. Bevor Sie sie aktivieren, sollten Sie die Advisor Core-Daten herunterladen, um die Netzwerk-Bandbreite zu minimieren.)
6 Stunden
12 Stunden
© 1999-2008 Novell, Inc. All rights reserved.
< Zurück
Weiter >
Abbrechen

12 Klicken Sie anschließend auf "Weiter".

Wichtig: Wenn Ihr Benutzername und Ihr Passwort nicht überprüft werden können, werden Sie gefragt, ob Sie fortfahren möchten.

Ab Sentinel 6.0 SP2 müssen die Anmeldedaten und das Passwort den zur Advisor-Berechtigung gehörenden Anmeldedaten und Passwort entsprechen. Eine häufige Fehlerquelle ist die Verwendung von falschen Novell-Anmeldedaten und dem falschen Passwort. Es kann sich zwar um gültige Novell-Anmeldedaten handeln, jedoch verfügen diese nicht über eine entsprechende Berechtigung bzw. gehören sie nicht zur Advisor-Lizenz.

---

13 Klicken Sie auf Installieren.

14 Nach der Installation werden Sie aufgefordert, neu zu booten oder sich erneut anzumelden und Sentinel Services manuell zu starten. Klicken Sie auf Fertig stellen, um das System neu zu booten.

Wichtig: Der geplante Advisor-Download kann erst nach dem erneuten Booten durchgeführt werden.

Tipp: Nach der Installation können Sie die Advisor-Email-Adressen ändern, indem Sie die Datei `advisor_client.xml` und im Verzeichnis „$ESEC_HOME/config“ bearbeiten. Weitere Informationen finden Sie unter “Registerkarte „Advisor“” im *Sentinel-Benutzerhandbuch*.

4.3.1 Laden von Daten

Auch wenn das erstmalige Laden von Advisor-Daten über den geplanten Service („Direktes Herunterladen vom Internet“) oder manuell über die Option „Einzelplatzbetrieb“ durchgeführt werden kann, wird diese Vorgehensweise aufgrund der hohen Netzwerkbelastung nicht empfohlen. Deshalb sind die Skripte `advisor.sh` und `advisor.bat` ursprünglich standardmäßig deaktiviert. Aktivieren Sie die Skripte, nachdem die Daten mithilfe der Sentinel 6 Exploit Detection

geladen wurden und ein Snapshot der Advisor-Daten auf der Advisor Core-Daten-Festplatte erstellt wurde. Durch das Laden dieser Daten wird die erforderliche Zeit zum Aktualisieren der Datenbank erheblich reduziert. Auch die erforderliche Netzwerk-Bandbreite reduziert sich.

Die Advisor Core-Daten stehen auf dem Novell-Kundenserviceportal für Kunden zur Verfügung, die ein Jahresabonnement für Advisor erworben haben. Das ISO-Image umfasst weniger als 900 MB, lädt jedoch ca. 10 GB an Daten in die Advisor-Tabellen.

Das erstmalige Laden von Daten kann je nach den Spezifikationen der Computer und sonstigen Belastungen auf dem Datenbankserver bis zu einem Tag in Anspruch nehmen.

Nach dem erstmaligen Laden von Daten können inkrementelle Aktualisierungen manuell oder über die Funktion „Direktes Herunterladen vom Internet“ geladen werden.

Wichtig: Das Dateninstallationsprogramm für Advisor funktioniert nur mit Sentinel 6.0 SP2 und höher, nachdem die entsprechenden Datenbank-Patches im Rahmen des Patch-Installationsvorgangs angewendet wurden. Der Aufrüstungsvorang und das Dateninstallationsprogramm erstetzen alle Advisor-Daten, die vor Sentinel 6.0 SP2 heruntergeladen wurden.

So laden Sie einen Daten-Snapshot von Advisor herunter:

1. Melden Sie sich unter Solaris/Linux als Benutzer „root“ bzw. unter Windows als Administratorbenutzer an.
2. Legen Sie den Sentinel 6 Advisor Core Data-Installationsdatenträger ein und mounten Sie ihn.
3. Starten Sie das Installationsprogramm. Wechseln Sie dazu in das Installationsverzeichnis auf der CD-ROM und gehen Sie dann wie folgt vor:
   - Unter Solaris/Linux: Führen Sie `advisor_bcp_in.sh` aus.
   - Unter Windows: Führen Sie `advisor_bcp_in.bat` aus.
4. Geben Sie an der Konsole den entsprechenden DB-Berechtigungsnachweis an:
   - Unter Linux geben Sie den Datenbank-Benutzernamen (Standard: „esecdba“) und die Oracle-SID (Instanzname) an.
   - Unter Windows geben Sie den Datenbank-Hostnamen, den Datenbanknamen (Standard: ESEC) und den Authentifizierungsmodus für die Datenbank an. Bei Verwendung von SQL-Authentifizierung müssen Sie außerdem den Datenbankbenutzernamen (Standard: „esecdba“) und das Passwort angeben.
5. Geben Sie an, wie lang die Pause in Sekunden zwischen der Verarbeitung der einzelnen Dateien sein soll. Der Standardwert ist 0 Sekunden, doch dieser Wert kann bei hoher Datenbankbelastung erhöht werden, um eine Pause zwischen der Verarbeitung der Datendateien einzuführen.
6. Um die Effizienz des Ladevorgangs zu erhöhen, deaktiviert das System Indizes und Beschränkungen für die Advisor-Tabellen und schneidet die Advisor-Tabellen ab. Die folgende Meldung wird angezeigt:

```
Disabling indexes on the Advisor tables…
Successfully disabled indexes on the Advisor tables
Disabling constraints on the Advisor tables...
Successfully disabled constraints on the Advisor tables
Truncating Advisor tables...
Successfully truncated Advisor tables
```

7 Das Advisor-Skript wird gestartet und die Massendaten werden in die entsprechende Tabelle eingespeist. Der Snapshot der Daten wird in der Datenbank gespeichert.

8 Nachdem alle Dateien im Snapshot geladen wurden, werden die Beschränkungen wieder aktiviert, die Indizes neu erstellt und die folgenden Meldungen werden angezeigt:

```
Successfully enabled constraints on the Advisor tables
Successfully rebuilt indexes on the Advisor tables
```

9 Nach Abschluss des Massen-Feeds zeigt das System eine Meldung über den erfolgreichen Abschluss an.

10 Aktivieren Sie die inkrementalen Datenaktualisierungen für Advisor.

Es sollten regelmäßige inkrementelle Datenaktualisierungen für Advisor eingeplant werden (entweder automatisch geplant mithilfe von „Direktes Herunterladen vom Internet“ oder manuell mit der Option „Einzelplatzbetrieb“), um die Advisor-Datenbank auf den neusten Stand zu bringen und dort zu halten.

4.3.2 Aktivieren von Advisor-Aktualisierungen

Um große Netzwerkauslastungen zu vermeiden, sind die inkrementalen Advisor-Downloads standardmäßig deaktiviert. Aktivieren Sie die Downloads, nachdem die Advisor Core-Daten geladen wurden.

So aktivieren Sie Advisor-Downloads:

1 Öffnen Sie die Datei `advisor.sh` oder `advisor.bat` zur Bearbeitung.

Unter Linux: $ESEC_HOME/bin/advisor.sh

Unter Windows: %ESEC_HOME%\bin\advisor.bat

2 **Für Linux:**

Setzen Sie zum Auskommentieren eine Raute (#) vor den exit-Befehl am Anfang der Datei.

```
# exit
```

Für Windows:

Geben Sie zum Auskommentieren vor den exit-Befehl am Anfang der Datei „rem“ (ohne Anführungszeichen) ein.

```
rem exit
```

3 Datei speichern.

Beim nächsten geplanten oder manuellen Download sollten die Daten wie erwartet geladen werden.

4.3.3 Verbindung mit dem Advisor-Server über einen Proxy

Um für das Herunterladen von Feeds eine Verbindung mit dem Advisor-Server über einen Proxy herzustellen, müssen Sie die Advisor-Konfiguration aktualisieren. Dafür kann es erforderlich sein, bis zu vier neue Eigenschaften zu jeder `container.xml`-Datei hinzuzufügen, die vom Advisor verwendet wird. Wenn für den Proxyserver keine Authentifizierung erforderlich ist, müssen Sie lediglich die Host- und Portinformationen des Proxyservers hinzufügen. Wenn für den Proxyserver Authentifizierung erforderlich ist, müssen Sie außerdem den Benutzernamen und das Passwort für den Proxyserver hinzufügen.

So konfigurieren Sie Advisor:

1. Installieren Sie Advisor im Modus für direkte Verbindungen. Da das aktuelle Installationsprogramm Verbindungen über einen Proxyserver nicht unterstützt, scheitert die vom Installationsprogramm durchgeführte Authentifizierungsprüfung. Sie müssen dennoch mit der Installation fortfahren.
2. Wechseln Sie in den Ordner `%ESEC_HOME%\sentinel\config`.
3. Öffnen Sie `advisor_client.xml` und fügen Sie folgende Zeilen zum Abschnitt „DownloadComponent“ hinzu

   ```
   <property name="proxy_host">proxyHost</property>
   <property name="proxy_port">proxyPort</property>
   ```

   Fügen Sie außerdem folgende Eigenschaften hinzu, wenn für den Proxyserver Authentifizierung erforderlich ist.

   ```
   <property name="proxy_username">proxyUser</property>
   <property name="proxy_password" />
   ```
4. Wenn für den Proxyserver Authentifizierung erforderlich ist, gehen Sie wie folgt vor:
   - Kopieren Sie die Datei `proxy_password_update.bat` in den „Ordner %ESEC_HOME%\sentinel\bin“.
   - Um die Advisor-Containerdaten mit dem Proxy-Benutzerpasswort zu aktualisieren, müssen Sie folgenden Befehl ausführen: `%ESEC_HOME%\sentinel\bin\proxy_password_update.bat proxyPasswd`.
   - Vergewissern Sie sich, dass `advisor_client.xml` nun das verschlüsselte Proxypasswort enthält.
5. Führen Sie `advisor.bat` aus, um Advisor-Daten herunterzuladen und zu verarbeiten. Sie können sich vergewissern, dass Advisor eine Verbindung über den Proxyserver herstellen kann, indem Sie folgende Protokolldateien überprüfen: `%ESEC_HOME%\sentinel\log\Advisor_0.0.log` und `%ESEC_HOME%\sentinel\log\advisor.log`

4.4 Advisor-Berichte

Crystal Reports Server™ ist das Berichterstellungswerkzeug, das mit Sentinel zusammenarbeitet.

So führen Sie Crystal-Berichte für Advisor aus:

- Installieren und konfigurieren Sie Crystal Server. Weitere Informationen zur Installation von Crystal Reports Server finden Sie unter Kapitel 8, „Crystal Reports für Windows“, auf Seite 101 undKapitel 9, „Crystal Reports für Linux“, auf Seite 131.
- Veröffentlichen Sie Advisor Crystal Reports auf Crystal Server.

4.4.1 Konfiguration von Advisor-Berichten

Zur Ausführung von Advisor-Berichten müssen Sie die Konfigurationsschritte für Crystal Reports Server für Windows bzw. Linux ausführen und die Advisor-URL für Berichte konfigurieren. Weitere Informationen zum Importieren von Berichtsschablonen und zum Konfigurieren des Sentinel Control Center für die Anzeige der Advisor-Berichte erhalten Sie unter: Kapitel 8, „Crystal Reports für Windows“, auf Seite 101 und Kapitel 9, „Crystal Reports für Linux“, auf Seite 131.

4.5 Wartung von Advisor

Im Sentinel-Benutzerhandbuch sind mehrere Wartungsaufgaben für Advisor beschrieben:

- Manuelle Aktualisierung der Advisor-Daten: Um wirksam zu sein, müssen die Advisor-Daten regelmäßig aktualisiert werden, da immer neue Angriffe und Anfälligkeiten zum Datenfeed hinzugefügt werden. Wenn diese Aktualisierungen nicht über „Direktes Herunterladen vom Internet“ geplant sind, müssen sie manuell durchgeführt werden.
- Änderung des Passworts, das Advisor für automatische Datenaktualisierungen verwendet (sofern erforderlich)
- Änderung der Konfiguration für Advisor-Benachrichtigungs-Emails
- Änderung des Zeitpunkts für die geplante Datenaktualisierung

Weitere Informationen zu diesen Wartungsaufgaben finden Sie im Abschnitt “Wartung von Advisor” im *Sentinel-Benutzerhandbuch*.

Testen der Installation

5

- Abschnitt 5.1, „Testen der Installation“, auf Seite 77
- Abschnitt 5.2, „Bereinigen nach Testen“, auf Seite 84
- Abschnitt 5.3, „Einführung“, auf Seite 85

5.1 Testen der Installation

Sentinel wird mit einem Demonstrations-Collector installiert, mit dem viele der Grundfunktionen des Systems getestet werden können. Mit diesem Collector können Sie aktive Ansichten, die Erstellung von Vorfällen, Korrelationsregeln und Berichte testen. Folgendes Verfahren beschreibt die Schritte für das Testen des Systems und die erwarteten Ergebnisse. Möglicherweise werden bei Ihnen nicht genau dieselben Ereignisse angezeigt, Ihre Ergebnisse sollten jedoch in etwa mit den unten angezeigten Ergebnissen übereinstimmen.

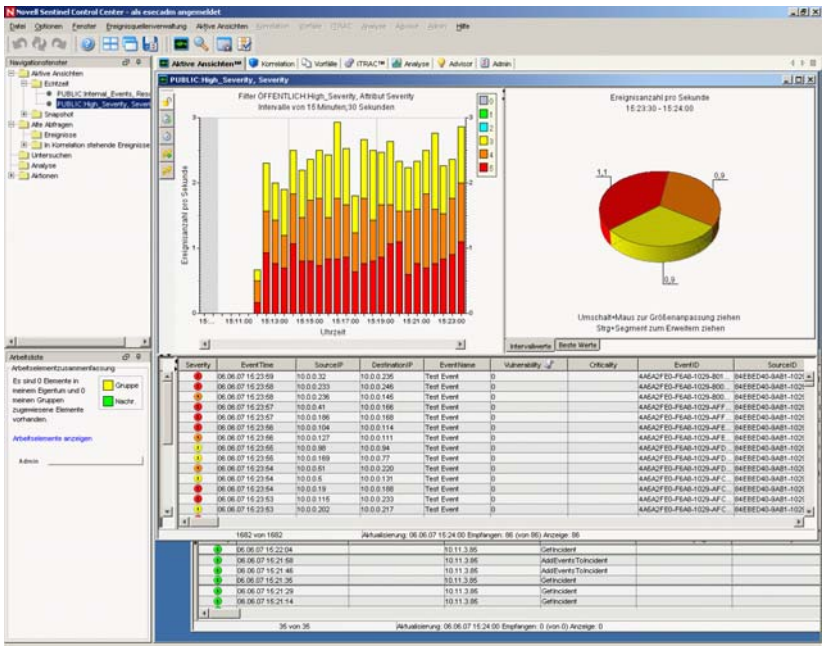
Mit diesen Test können Sie auf einer grundlegenden Ebene folgende Punkte überprüfen:

- Sentinel-Services werden ausgeführt.
- Die Kommunikation über den Nachrichten-Bus funktioniert.
- Interne Revisionsereignisse werden gesendet.
- Ereignisse können über einen Collection-Manager gesendet werden
- Ereignisse werden in die Datenbank eingefügt und können über „Alte Ereignisabfrage“ oder über die Crystal Reports abgerufen werden.
- Vorfälle können erstellt und angezeigt werden.
- Die Correlation Engine evaluiert Regeln und löst die zugehörigen Ereignisse aus.
- Sentinel Data Manager kann eine Verbindung mit der Datenbank herstellen und Partitionsinformationen lesen.

Wenn einer dieser Tests nicht erfolgreich ist, lesen Sie im Installationsprotokoll und den anderen Protokolldateien nach und nehmen Sie ggf. Kontakt mit Novell Technical Support (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) auf.

So testen Sie die Installation:

1. Doppelklicken Sie auf das Sentinel Control Center-Symbol auf dem Desktop.
2. Melden Sie sich als der Sentinel-Administratorbenutzer beim System an, der während der Installation angegeben wurde (Standard: „esecadm“) Das Sentinel Control Center wird geöffnet und die Registerkarte „Aktive Ansichten“ wird angezeigt. Dabei sind die Ereignisse mit den öffentlichen Filtern „Internal_Events” und „High_Severity” gefiltert.



3 Rufen Sie das Menü „Ereignisquellenverwaltung“ auf und wählen Sie die Option „Live-Ansicht“.

4 Klicken Sie in der grafischen Ansicht mit der rechten Maustaste auf „Ereignisquelle mit 5 EPS“ und wählen Sie die Option „Starten“.

5 Schließen Sie das Fenster „Live-Ansicht“ unter “Ereignisquellenverwaltung“.

6 Schließen Sie die Registerkarte „Aktive Ansichten“. Es wird ein aktives Fenster mit dem Titel „ÖFFENTLICH: High_Severity, Schweregrad“ angezeigt. Es kann einige Zeit dauern, bis der Collector (Sammelstelle) gestartet wird und die Daten in diesem Fenster angezeigt werden.

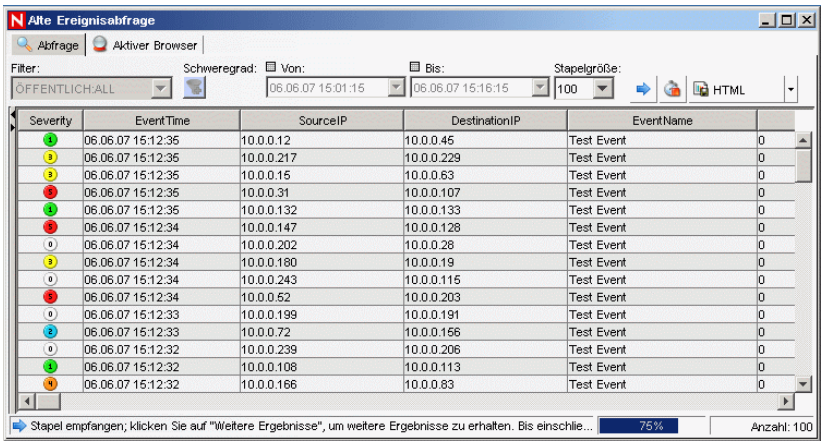
7 Klicken Sie in der Symbolleiste auf die Schaltfläche „Ereignisabfrage“. Das Fenster „Alte Ereignisabfrage“ wird angezeigt.

8 Klicken Sie im Fenster „Alte Ereignisabfrage“ auf den Abwärtspfeil zu „Filter“, um den Filter auszuwählen. Aktivieren Sie den Filter „Öffentlich: Alle“ und klicken Sie auf „Auswählen“.

9 Wählen Sie eine Zeitraum aus, der die Zeit abdeckt, in der der Collector aktiv war. Wählen Sie den Löschbereich mithilfe der Dropdown-Pfeile „Von“ und „Bis“ aus.

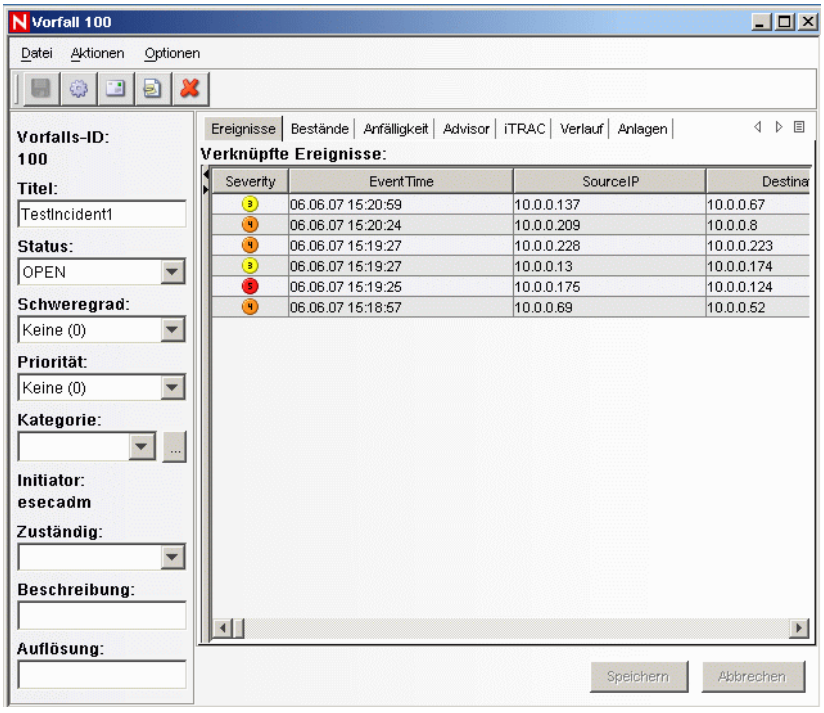
10 Wählen Sie eine Batchgröße aus dem Dropdown-Feld „Batchgröße“.

11 Klicken Sie auf das Symbol mit der Lupe, um die Abfrage auszuführen.



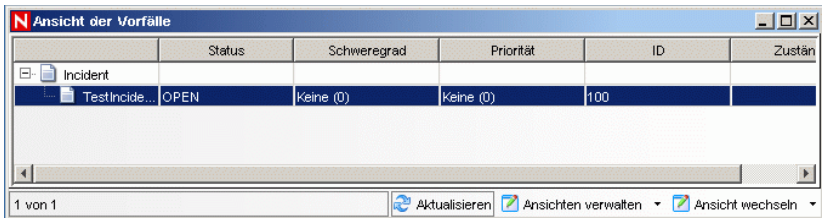
12 Wählen Sie bei gedrückter STRG- oder UMSCHALT-Taste mehrere Ereignisse aus dem Fenster „Alte Ereignisabfrage“ aus.

13 Klicken Sie mit der rechten Maustaste und wählen Sie „Vorfall erstellen“.

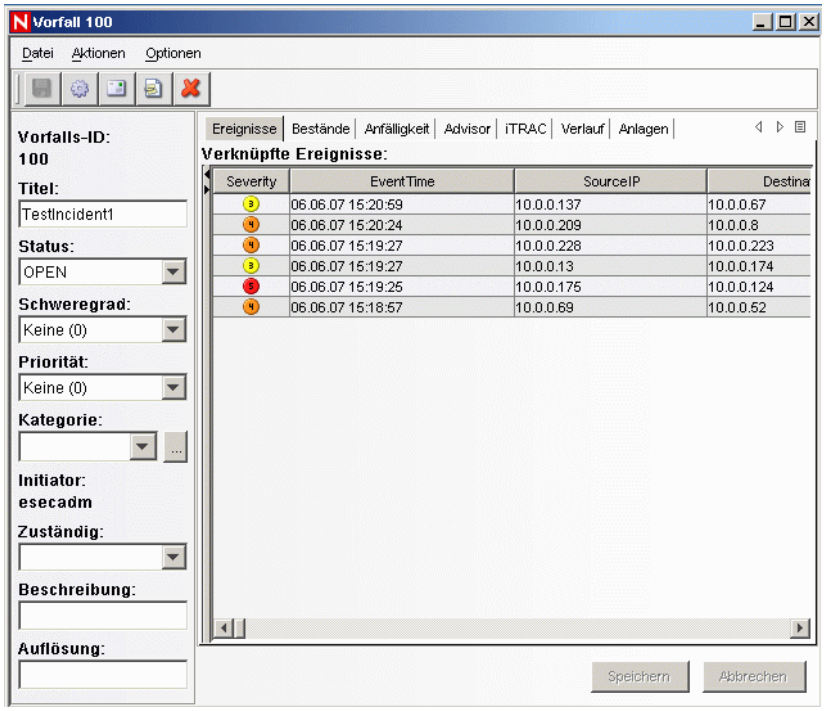


14 Benennen Sie den Vorfall „TestIncident1“ und klicken Sie auf „Erstellen“. Eine Erfolgsbenachrichtigung wird angezeigt. Klicken Sie auf „OK“.

15 Wählen Sie die Registerkarte „Vorfall“. Der Manager für die Vorfallansicht wird angezeigt. Im Manager für die Vorfallansicht wird der gerade erstellte Vorfall angezeigt.



16 Doppelklicken Sie auf den anzuzeigenden Vorfall.



17 Schließen Sie das Fenster „Vorfall“, wechseln Sie zu „Datei“ > „Beenden“ oder klicken Sie in der oberen rechten Ecke des Fensters auf „X“.

18 Klicken Sie auf den Karteireiter Analyse. Öffnen Sie den Ordner „Ereignisse“ im Analysennavigator.

19 Klicken Sie auf „Alte Ereignisabfragen“.

20 Klicken Sie auf „Analyse“ > „Bericht erstellen“ oder klicken Sie auf das Symbol „Bericht erstellen“. Das Fenster „Ereignisabfrage“ wird geöffnet. Legen Sie Folgendes fest:

- Zeitrahmen
- Filter
- Schweregrad
- Stapelgröße (Dies ist die Anzahl der angezeigten Ereignisse – ältere Ereignisse werden vor neueren Ereignissen angezeigt.)

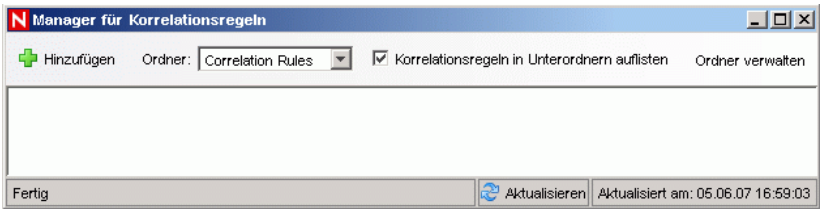
21 Klicken Sie auf das Symbol „Suche starten“.

22 Klicken Sie zum Anzeigen des nächsten Ereignisstapels auf Weitere Optionen.

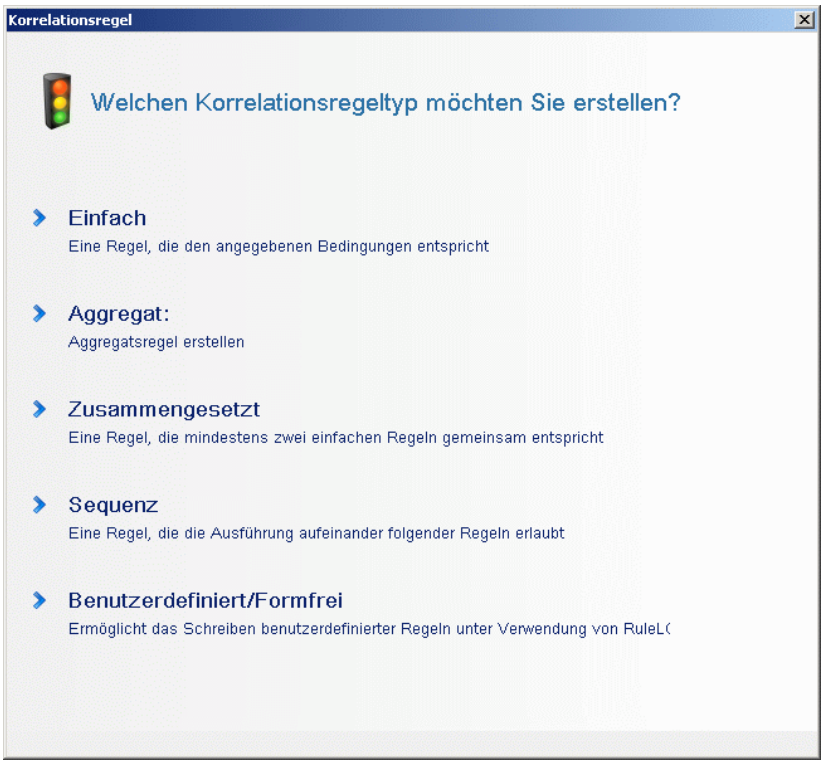
23 Ordnen Sie die Spalten neu an, indem Sie diese ziehen und ablegen, und ändern Sie die Sortierreihenfolge, indem Sie auf die Spaltenüberschrift klicken.

24 Wenn Ihre Abfrage fertig ist, wird sie im Navigator der Liste der Schnellabfragen hinzugefügt.

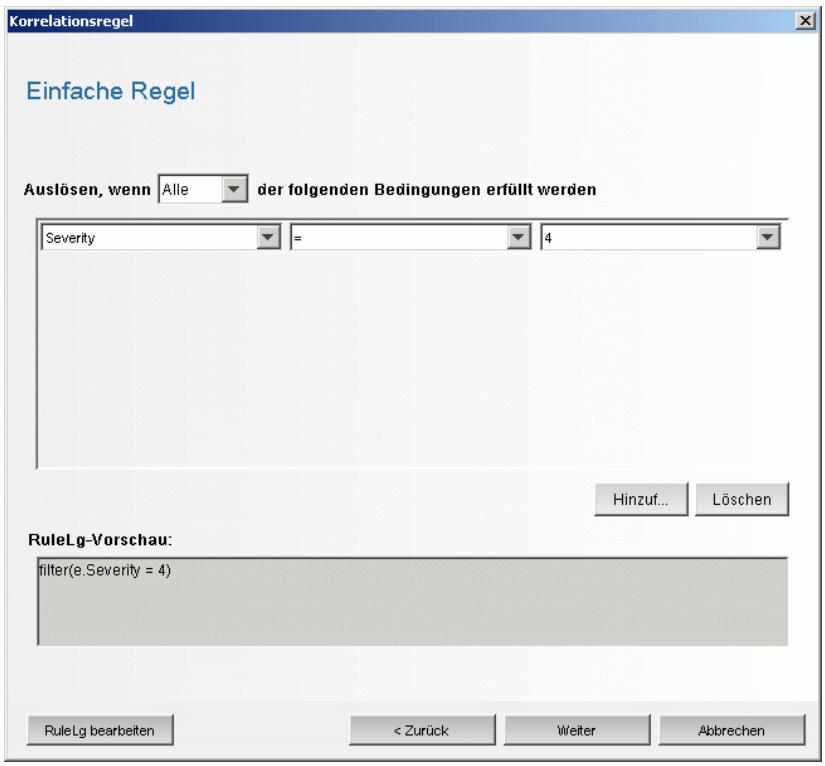
25 Öffnen Sie die Registerkarte „Korrelation“. Der Manager für Korrelationsregeln wird angezeigt.



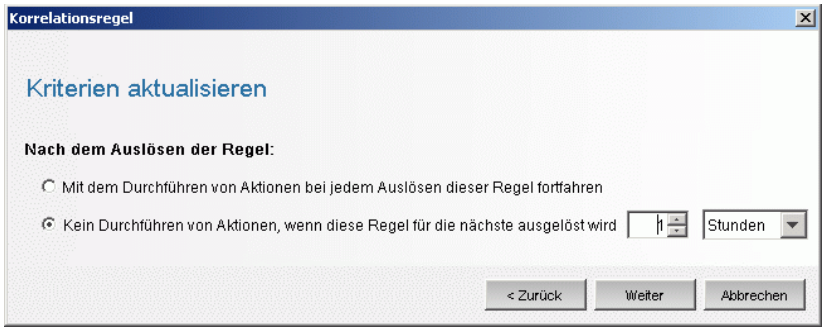
26 Klicken Sie auf Hinzufügen. Der Assistent für Korrelationsregeln wird angezeigt.



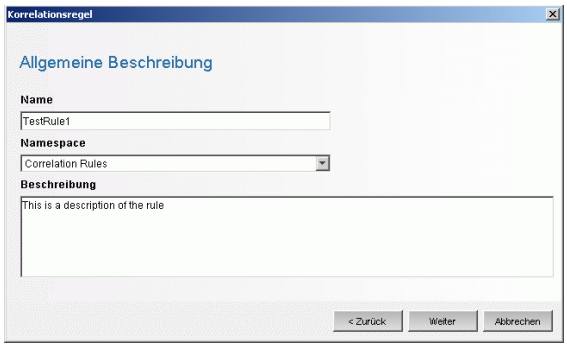
27 Klicken Sie auf „Einfach“. Das Fenster „Einfache Regel“ wird angezeigt.



28 Verwenden Sie die Dropdown-Menüs, um die Kriterien auf „Schweregrad = 4“ festzulegen. Klicken Sie anschließend auf "Weiter". Das Fenster „Kriterien aktualisieren“ wird angezeigt.



29 Wählen Sie „Kein Durchführen von Aktionen, wenn diese Regel für die nächste ausgelöst wird“ und verwenden Sie das Dropdown-Menü, um den Zeitraum auf 1 Minute festzulegen. Klicken Sie anschließend auf "Weiter". Das Fenster „Allgemeine Beschreibung“ wird angezeigt.

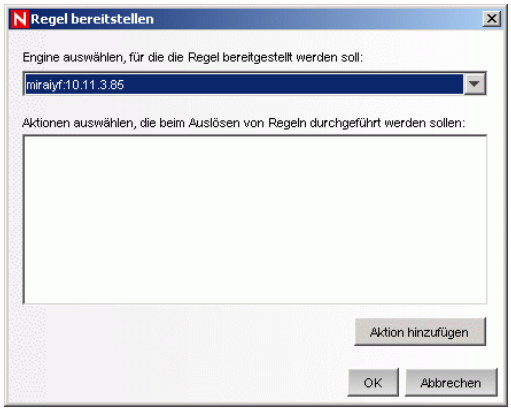


30 Geben Sie der Regel den Namen „Korrelationsregel“, geben Sie die Beschreibung an und klicken Sie auf „Weiter“.

31 Wählen Sie „Nein, erstellen Sie keine andere Regel“ aus und klicken Sie auf „Weiter“.

32 Öffnen Sie das Fenster „Manager für Korrelationsregeln“.

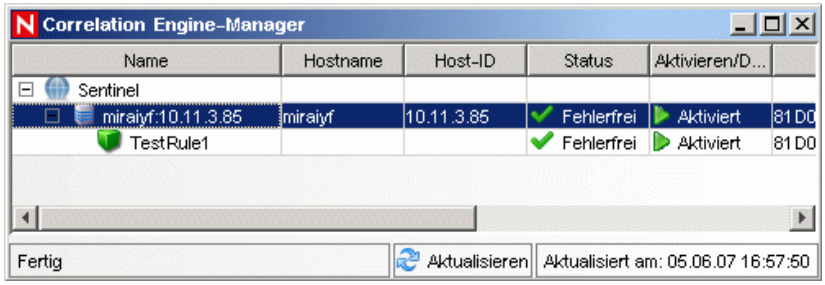
33 Heben Sie eine Regel hervor und klicken Sie auf den Link „Bereitstellungsregeln“. Das Fenster „Regel bereitstellen“ wird angezeigt.



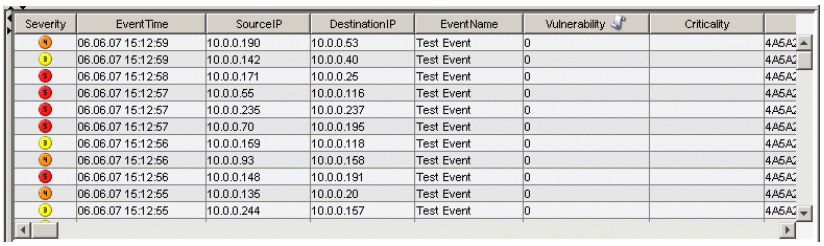
34 Wählen Sie im Fenster „Regel bereitstellen“ die Engine aus der Dropdown-Liste aus, für die die Regel bereitgestellt werden soll.

35 Wählen Sie eine Aktion „Email senden“ aus, die der Regel zugeordnet werden soll, und klicken Sie auf „OK“. Eine Aktion muss vor dem Zuordnen in Sentinel erstellt werden.

36 Wählen Sie den Correlation Engine-Manager aus. Sie können unter der Correlation Engine sehen, dass die Regel bereitgestellt/aktiviert wurde.



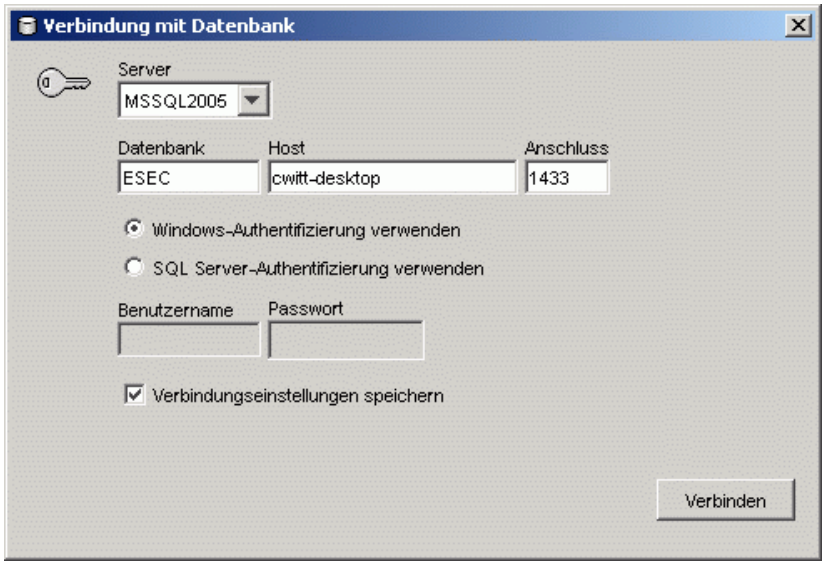
37 Wechseln Sie zur Registerkarte „Aktive Ansichten“ und überprüfen Sie, ob das korrelierte Ereignis generiert wurde.



38 Schließen Sie das Sentinel Control Center.

39 Doppelklicken Sie auf dem Desktop auf das Symbol „Sentinel Data Manager (SDM)“.

40 Melden Sie sich bei SDM mithilfe des verwaltungsbefugten Datenbankbenutzers an, der während der Installation angegeben wurde (standardmäßig „esecdba“).



41 Klicken Sie auf jede Registerkarte, um zu überprüfen, ob Sie darauf zugreifen können.

42 Schließen Sie Sentinel Data Manager.

Wenn Sie alle diese Schritte ohne Fehler durchführen konnten, haben Sie eine allgemeine Überprüfung der Sentinel-Systeminstallation abgeschlossen.

5.2 Bereinigen nach Testen

Sie sollten nach dem Abschließen der Systemüberprüfung die für die Tests erstellten Objekte entfernen.

So führen Sie eine Bereinigung nach dem Testen des Systems durch

1 Melden Sie sich beim System mithilfe des verwaltungsbefugten Sentinel-Benutzers an, der während der Installation angegeben wurde (standardmäßig „esecadm“).

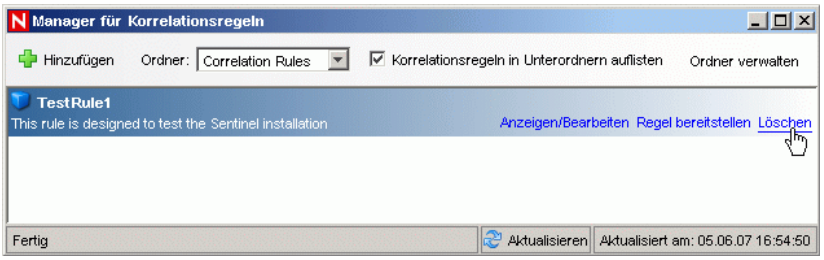
2 Wählen Sie die Registerkarte „Korrelation“.

3 Öffnen Sie den Correlation Engine-Manager.

4 Klicken Sie im Correlation Engine-Manager auf „TestRule1“ und wählen Sie “Bereitstellung aufheben“ aus.

5 Öffnen Sie den Correlation Rule Manager.

6 Wählen Sie „TestRule1“ aus und klicken Sie auf „Löschen“.



7 Wechseln Sie zum Menü „Ereignisquellenverwaltung“ und wählen Sie „Live-Ansicht“ aus.

8 Klicken Sie in der Hierarchie der grafischen Ereignisquelle mit der rechten Maustaste auf „Allgemeiner Collector“ und wählen Sie „Stoppen“ aus.

9 Schließen Sie das Fenster „Ereignisquellenverwaltung“.

10 Wählen Sie die Registerkarte „Vorfälle“.

11 Öffnen Sie den Manager für die Vorfallansicht.

12 Wählen Sie„TestIncident1“ aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Löschen“ aus.

5.3 Einführung

Zum Starten mit echten Daten müssen Sie Collectors importieren und konfigurieren, die für Ihre Umgebung passend sind, Ihre eigenen Regeln erstellen, iTRAC-Workflows erstellen usw. Mit Sentinel Solution Packs können Sie schnell anfangen.

Hinzufügen von Sentinel-Komponenten

6

- Abschnitt 6.1, „Hinzufügen von Sentinel-Komponenten zu einer bestehenden Installation“, auf Seite 87
- Abschnitt 6.2, „Installieren zusätzlicher Lastausgleichsknoten“, auf Seite 87

6.1 Hinzufügen von Sentinel-Komponenten zu einer bestehenden Installation

Manchmal kann es erforderlich sein, zusätzliche Sentinel-Komponenten auf einem Computer zu installieren, auf dem bereits eine Sentinel-Installation vorhanden ist. Möglicherweise müssen Sie beispielsweise den Collector Builder installieren, wo das Sentinel Control Center bereits installiert wurde.

Mit dem Sentinel-Installationsprogramm ist diese Art der Installation einfach. Vergewissern Sie sich zunächst, dass die Voraussetzungen für die Installation einer zusätzlichen Komponente entsprechend der Kapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31 erfüllt sind. Die Anforderungen auf dem Computer erhöhen sich wahrscheinlich beim Installieren zusätzlicher Komponenten. Führen Sie anschließend das Sentinel-Installationsprogramm so auf dem Zielcomputer aus, als ob Sie die Installation auf einem „leeren“ Computer ausführen würden. Beim Ausführen im Modus zum Hinzufügen von Komponenten verändert das Installationsprogramm sein Verhalten leicht auf folgende Weise:

- Das Installationsprogramm ermittelt automatisch die vorhandene Sentinel-Installation und zeigt einen Bildschirm an, in dem der Speicherort der vorhandenen Installation sowie die bereits installierten Komponenten angegeben werden.
- Das Installationsprogramm fordert nicht zur Eingabe des Zielverzeichnisses auf. Es wird das Zielverzeichnis der vorhandenen Installation verwendet.
- Das Installationsprogramm fordert nicht zur Auswahl des einfachen oder benutzerdefinierten Installationstyps auf. Es wird vom benutzerdefinierten Installationstyp ausgegangen.

Hinweis: In einer verteilten Sentinel-Installation kann nur eine Instanz von Advisor und Communication Server vorhanden sein.

6.2 Installieren zusätzlicher Lastausgleichsknoten

Manchmal ist es notwendig, einen zusätzlichen Sentinel-Verarbeitungsknoten für die verteilte Sentinel-Umgebung zu installieren, um zusätzlichen Lastausgleich über Computer hinweg zu laden. Wenn beispielsweise die Arbeitsspeicherauslastung auf einem Computer hoch ist, auf dem eine Correlation Engine ausgeführt wird, sollten Sie das Hinzufügen eines anderen Computers in Erwägung ziehen, auf dem die Correlation Engine ausgeführt wird. (Dafür ist eventuell eine weitere

Lizenz erforderlich.) Sie können dann die Korrelationsregeln auf diesen beiden Engines bereitstellen, um die Last auf einem einzelnen Computer zu reduzieren, wenn alle Regeln darauf bereitgestellt wurden.

Führen Sie dazu einfach das Installationsprogramm auf dem neuen Computer aus, wie in Kapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31 beschrieben. Geben Sie bei der Installation nur die Komponenten an, für die Sie zusätzliche Lastausgleichsknoten hinzufügen möchten. Für die folgenden Komponenten kann ein Lastausgleich durchgeführt werden:

- Correlation Engine
- Collector Manager
- DAS_Binary-Prozess

Der DAS_Binary-Prozess ist für das Einfügen der Ereignisdatenbank verantwortlich. Da durch das Einfügen von Ereignisdatenbanken ein Engpass beim Ereignisfluss verursacht werden kann, führt der Lastausgleich des DAS_Binary-Prozesses üblicherweise wieder zu einem erheblichen Leistungsgewinn, was den Durchsatz von Ereignissen pro Sekunde betrifft. Außerdem kann für die Correlation Engine- und Collector Manager-Komponenten ein Lastausgleich durchgeführt werden, indem Instanzen dieser Komponenten auf zusätzlichen Computern installiert werden.

6.2.1 Mehrere DAS_Binary-Prozesse

Obwohl es sich nicht um einen echten Lastausgleich handelt, ist es möglich, mehrere DAS_Binary-Instanzen in einem Sentinel-System zu konfigurieren, um die Leistung zu verbessern. DAS_Binary ist der Prozess, mit dem das Einfügen von Ereignissen in die Datenbank verwaltet wird, und die höchsten Ereignisraten, die Novell beim internen Testen erzielt hat, waren mit mehreren DAS_Binary-Prozessen. Weitere Informationen zum Testen der Leistung finden Sie auf der Novell-Dokumentations-Site (http://www.novell.com/documentation/sentinel61).

Mehrere DAS_Binary-Prozesse können auf demselben Computer installiert oder über mehrere Computer verteilt werden.

So konfigurieren Sie DAS_Binary-Instanzen auf verschiedenen Computern:

1. Verwenden Sie das Sentinel-Installationsprogramm, um die DAS-Komponente auf jedem der Computer zu installieren, auf dem ein DAS_Binary-Prozess ausgeführt wird. Alle DAS_Binarys sollten mit derselben Datenbank verbunden werden. Geben Sie deshalb während der Installation dieselben Informationen für die Datenbankverbindung an, die Sie für die erstmalige DAS-Installation angegeben haben.
2. Nehmen Sie bei allen Computern, auf denen Sie DAS_Binary ausführen möchten, die folgenden Änderungen vor:
   - **2a** Melden Sie sich als „esecadm“ (unter UNIX) oder als Administrator (unter Windows) auf einem der Computer an, auf dem mehrere Instanzen des DAS_Binary-Prozesses ausgeführt werden, und suchen Sie die Datei `configuration.xml` im Verzeichnis „$ESEC_HOME/config“ („%ESEC_HOME%\config“ unter Windows).
   - **2b** Fügen Sie die folgenden Informationen dem Abschnitt „Services“ der Datei `configuration.xml` hinzu:
     ```
     <service name="DAS_Binary_EventStore" plugins=""
     strategyid="sentinel_client" subscriptiongroup="dasbin" />
     ```
   - **2c** Speichern Sie die Datei `configuration.xml`.

3 Nehmen Sie auf den Computern, auf denen sekundäre DAS_Binary-Prozesse ausgeführt werden, die folgenden Änderungen vor. Ein sekundäres DAS_Binary ist eines, das nicht auf dem Haupt-Sentinel-Server ausgeführt wird.

3a Entfernen Sie die Datei `sentinelhost.id` aus dem Verzeichnis „$ESEC_HOME/data“ („%ESEC_HOME%\data“ unter Windows). Dadurch wird der Collector Manager auf diesem Computer gezwungen, eine neue ID zu generieren, anstatt die selbe ID zu verwenden, die der Collector Manager von Sentinel-Server verwendet.

3b Die anderen DAS-Prozesse sollten deaktiviert werden. Legen Sie hierfür im Prozessabschnitt der Datei `configuration.xml` auf den ausschließlichen DAS_Binary-Computern das Attribut „min_instances“ wie folgt fest:

`min_instances=”0”`

für die folgenden Prozesseinträge:

- DAS_RT
- DAS_Aggregation
- DAS_Query
- DAS_ITRAC

4 Der sekundäre Sentinel-Dienst sollte verwendet werden. Deshalb muss die Datei `sentinel.conf` im Verzeichnis „ESEC_HOME/config“ geändert werden, indem die folgende Zeile durch Entfernen des #-Zeichens vom Anfang der Zeile auskommentiert wird:

`wrapper.app.parameter.1=../config/sentinel.xml`

und Auskommentieren der folgenden Zeile durch Einfügen des #-Zeichens am Anfang der Zeile:

`#wrapper.app.parameter.1=../config/sentinel_primary.xml`

5 Nehmen Sie die folgenden Änderungen an der Datei `das_binary.xml` auf einem der Computer vor, auf dem ein DAS_Binary-Prozess ausgeführt wird:

5a Erstellen Sie eine Kopie der gesamten DispatchManager-Komponente und ändern Sie die ID der neuen Komponente von „DispatchManager“ in „EventStoreDispatchManager“. Nach dieser Änderung sollten eine Komponente mit der ID „DispatchManager“ und eine Komponente mit der ID „EventStoreDispatchManager“ vorhanden sein. Nachfolgend finden Sie ein Beispiel dafür, wie die neue EventStoreDispatchManager-Komponente aussehen sollte.

5b Aktualisieren Sie den Wert der Eigenschaft mit Namen `esecurity.communication.service` der EventStoreDispatchManager-Komponente auf „DAS_Binary_EventStore“.

5c Entfernen Sie die Eigenschaft mit Namen `handler:esecurity.event.create` aus der DispatchManager-Komponente.

5d Entfernen Sie alle Eigenschaften mit einem Namen, der mit „handler:*“ beginnt, außer `handler:esecurity.event.create` aus der EventStoreDispatchManager-Komponente. Die Behandlungsroutine `handler:esecurity.event.create` sollte die einzige in der EventStoreDispatchManager-Komponente definierte Behandlungsroutine sein.

5e Fügen Sie der EventStoreService-Komponente das folgende XML-Element hinzu:

```
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

5f Speichern Sie die Datei `das_binary.xml`.

6 Kopieren Sie die Datei `das_binary.xml` auf alle Computer, auf denen ein DAS_Binary-Prozess ausgeführt wird. Hier finden Sie den Auszug eines Beispiels der Datei `das_binary.xml`, der die EventStoreDispatchManager-Komponente zeigt.

```
<obj-component id="EventStoreDispatchManager">
<class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</class>
<property
name="esecurity.communication.service">DAS_Binary_EventStore</
property>
<property name="dependencies">DAS_Query</property>
<property
name="handler:esecurity.event.create">esecurity.ccs.cracker.EventC
racker@ewizard_binary_event,correlation_binary_event,database_bina
ry_event,database_tagged_event,correlation_binary_event_update</
property>
<obj-component id="DispatcherStatsService">
<class>esecurity.ccs.comp.dispatcher.stats.DispatcherStatsManager<
/class>
<property name="ReportIntervals">900,3600,14400,86400</property>
<property name="MinLogReportInterval">900</property>
<property name="MinPublishReportInterval">86400</property>
<property name="ReportByServiceName">true</property>
<property name="ReportByMethodName">true</property>
<obj-component-ref>
<name>EventPublisher</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>
</obj-component>
```

Hier finden Sie den Auszug eines Beispiels der Datei `das_binary.xml`, der die EventStoreService-Komponente zeigt.

```
<obj-component id="EventStoreService">
<class>esecurity.ccs.comp.event.EventStoreService</class>
<property name="handler">esecurity.event.create</property>
<property name="waitBlocked">true</property>
<property name="maxThreads">6</property>
<property name="minThreads">6</property>
<property name="maxThreadsQueued">10</property>
<property name="queueSize">1000000</property>
<obj-component-ref>
<name>ThreadPool</name>
<ref-id>EventStoreThreadPool</ref-id>
</obj-component-ref>
<obj-component-ref>
```

```
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
<obj-component id="Persistor">
<class>esecurity.ccs.comp.event.jdbc.JDBCEventStore</class>
<property name="insert.batchsize">600</property>
<property
name="insert.strategy">esecurity.ccs.comp.event.jdbc.JDBCLoadStrat
egy</property>
<property name="insert.oci.workerCount">5</property>
<property name="insert.oci.queueWaitTime">1</property>
<property name="insert.oci.highWatermark">10000000</property>
<property name="insert.oci.lowWatermark">9000000</property>
<property name="insert.oci.optimizationFlag">on</property>
<property name="insert.pmaxWarningTime">300</property>
<property name="insert.pminWarningTime">300</property>
</obj-component>
<obj-component-ref>
<name>EventRedirect</name>
<ref-id>EventFileRedirectService</ref-id>
</obj-component-ref>
</obj-component>
```

7 Starten Sie den Sentinel-Dienst zum Aktivieren der Änderungen auf allen Computern neu, auf denen Sie die Änderungen vorgenommen haben.

Unter UNIX:

```
$ESEC_HOME/bin/sentinel.sh restart
```

Unter Windows:

```
Restart the "Sentinel" service using the Windows Service Manager.
```

So konfigurieren Sie mehrere DAS_Binary-Instanzen auf demselben Computer:

1 Melden Sie sich als „esecadm“ (unter UNIX) oder als Administrator (unter Windows) auf dem Computer an, auf dem mehrere Instanzen der DAS_Binary-Prozesse ausgeführt werden, und suchen Sie die Datei `configuration.xml` im Verzeichnis „$ESEC_HOME/config“ („%ESEC_HOME%\config“ unter Windows).

2 Suchen Sie in der Datei `configuration.xml` nach dem Abschnitt der XML-Datei, der die Diensteinträge definiert (siehe Beispiel unten). Machen Sie eine Kopie des DAS_Binary-Diensteintrags für jede Instanz von DAS_Binary, die Sie ausführen möchten. Erstellen Sie beispielsweise zum Ausführen zweier DAS_Binary-Prozesse zwei Kopien des DAS_Binary-Diensteintrags. Löschen Sie das Attribut „uuid“ für jeden der Diensteinträge (das Attribut „uuid“ wird beim Starten von Sentinel automatisch neu generiert). Nachfolgend finden Sie ein Beispiel für einen DAS_Binary-Diensteintrag.

```
<service name="DAS_Binary" plugins="" strategyid="sentinel_client"
uuid="4DA52BE0-E7A4-1029-BB2F-00132168CBDF"/>
```

3 Erstellen Sie in der Datei`configuration.xml` eine Kopie der folgenden DAS_Binary_EventStore-Diensteintrags-XML-Datei für jede Instanz von DAS_Binary, die Sie ausführen möchten. Dieser Dienst ist in der Datei `configuration.xml` nicht vorhanden, sodass Sie ihn aus dem Beispiel unten kopieren sollten. Erstellen Sie beispielsweise zum Ausführen zweier DAS_Binary-Prozesse zwei Kopien des folgenden DAS_Binary_EventStore-Diensteintrags:

```
<service name="DAS_Binary_EventStore" plugins=""
strategyid="sentinel_client" subscriptiongroup="dasbin" />
```

4 Geben Sie jeder Kopie von DAS_Binary und des DAS_Binary_EventStore-Diensteintrags einen eindeutigen Namen. So könnten die Dienstnamen beispielsweise DAS_Binary1“, „DAS_Binary_EventStore1“, „DAS_Binary2“ und „DAS_Binary_EventStore2“ lauten.

5 Suchen Sie nach dem Abschnitt der Datei `configuration.xml`, der die Prozesseinträge definiert (siehe Beispiel unten). Erstellen Sie eine Kopie des DAS_Binary-Prozesseintrags für jede Instanz von DAS_Binary, die Sie ausführen möchten. Erstellen Sie beispielsweise zum Ausführen zweier DAS_Binary-Prozesse zwei Kopien des DAS_Binary-Prozesseintrags. Ändern Sie für jeden DAS_Binary-Prozesseintrag Abschnitte des Eintrags wie unten beschrieben:

- **DAS_Binary Dsrv_name:** Führen Sie für eine Übereinstimmung mit den in Schritt 4 definierten DAS_Binary-Dienstnamen eine Änderung durch, beispielsweise„DAS_Binary2“.
- **DAS_Binary-Kommunikationsdienstname:** Geben Sie den folgenden Text in das Imageattribut des Prozesseintrags an dem Speicherort ein, der in fett im Beispiel für den Prozesseintrag unten angegeben ist. Ersetzen Sie für jeden DAS_Binary-Prozesseintrag den Teil „DAS_Binary“ des Texts unten mit dem zugeordneten Dienstnamen, beispielsweise „DAS_Binary2“.

  `-Desecurity.communication.service=DAS_Binary`
- **`das_binary.xml`-Dateiname:** Verwenden Sie einen beliebigen eindeutigen Namen, beispielsweise `das_binary_2.xml`. Diese Namen werden in einem späteren Schritt verwendet.
- **das_binary_log_prop-Dateiname:** Verwenden Sie einen beliebigen eindeutigen Namen, beispielsweise `das_binary_log_2.prop`. Diese Namen werden in einem späteren Schritt verwendet.
- **das_binary.cache-Verzeichnisname:** Verwenden Sie einen beliebigen eindeutigen Namen, beispielsweise `das_binary2.cache`. Jede Instanz von DAS_Binary muss einen anderes `das_binary.cache`-Verzeichnis verwenden.
- **DAS_Binary-Prozessname:** Ändern Sie für eine Übereinstimmung mit den in Schritt 4 definierten DAS_Binary-Dienstnamen den Wert des Prozesseintragsnamen, beispielsweise„DAS_Binary2“.

Die folgende XML-Datei ist ein Beispiel eines Prozesseintrags wie in den Anweisungen oben erläutert:

```
process component="DAS" depends="UNIX Communication Server,Windows
Communication Server" image="&amp;quot;$(ESEC_JAVA_HOME)/java&amp;quot; -
server -Dsrv_name=DAS_Binary -Xmx160m -Xms64m -XX:+UseParallelGC -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log/
DAS_Binary.hprof -Xss136k -Xrs -
Desecurity.communication.service=DAS_Binary -Duser.language=en  -
Djava.net.preferIPv4Stack=true -Dfile.encoding=UTF8 -
Desecurity.cache.directory=../data/das_binary.cache -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_binary_log.prop -
Dcom.esecurity.configurationfile=../config/configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../config/krb5.conf -jar ../lib/
```

```
ccsbase.jar ..//config//das_binary.xml" min_instances="1"
name="DAS_Binary" post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data"/>
```

6 Speichern Sie die Datei `configuration.xml`.

7 Suchen Sie die Datei `das_binary.xml` im Verzeichnis „$ESEC_HOME/config“ („%ESEC_HOME%\config“ unter Windows).

8 Erstellen Sie eine Kopie der Datei `das_binary.xml` für jede Instanz von DAS_Binary, die Sie ausführen möchten. Erstellen Sie beispielsweise zum Ausführen zweier Instanzen von DAS_Binary zwei Kopien von `das_binary.xml`.

9 Benennen Sie die kopierten `das_binary.xml`-Dateien so um, dass sie mit den in Schritt 5 ausgewählten Namen übereinstimmen.

10 Nehmen Sie an jeder der `das_binary.xml`-Dateien die folgenden Änderungen vor:

- Erstellen Sie eine Kopie der gesamten DispatchManager-Komponente und ändern Sie die ID der neuen Komponente von „DispatchManager“ in „EventStoreDispatchManager“. Nach dieser Änderung sollte eine Komponente mit der ID „DispatchManager“ und eine Komponente mit der ID „EventStoreDispatchManager“ vorhanden sein.
- Aktualisieren Sie den Wert mit Namen `esecurity.communication.service` der DispatchManager-Komponente mit dem entsprechenden Namen für DAS_Binary, beispielsweise „DAS_Binary2“.
- Aktualisieren Sie den Wert mit Namen `esecurity.communication.service` der EventStoreDispatchManager-Komponente mit dem entsprechenden Namen für DAS_Binary_EventStore, beispielsweise „DAS_Binary_EventStore2“.
- Entfernen Sie die Eigenschaft mit Namen `handler:esecurity.event.create` aus der DispatchManager-Komponente.
- Entfernen Sie alle Eigenschaften mit einem Namen, der mit „handler:*“ beginnt, außer handler:esecurity.event.create aus der EventStoreDispatchManager-Komponente. Die Behandlungsroutine `handler:esecurity.event.create` sollte die einzige in der EventStoreDispatchManager-Komponente definierte Behandlungsroutine sein.
- Fügen Sie der EventStoreService-Komponente das folgende XML-Element hinzu:

```
<obj-component-ref>
   <name>DispatchManager</name>
   <ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

11 Speichern Sie die `das_binary.xml`-Dateien.

12 Suchen Sie die Datei `das_binary_log.prop` im Verzeichnis „$ESEC_HOME/config“ („%ESEC_HOME%\config“ unter Windows).

13 Erstellen Sie eine Kopie der Datei `das_binary_log.prop` für jede Instanz von DAS_Binary, die Sie ausführen möchten. Erstellen Sie beispielsweise zum Ausführen zweier Instanzen von DAS_Binary zwei Kopien von `das_binary_log.prop`.

14 Benennen Sie die kopierten `das_binary_log.prop`-Dateien so um, dass sie mit den in Schritt 5 ausgewählten Namen übereinstimmen.

15 Starten Sie den Sentinel-Dienst neu, um die Änderungen zu aktivieren.

Unter UNIX:

```
$ESEC_HOME/bin/sentinel.sh restart
```

Unter Windows:

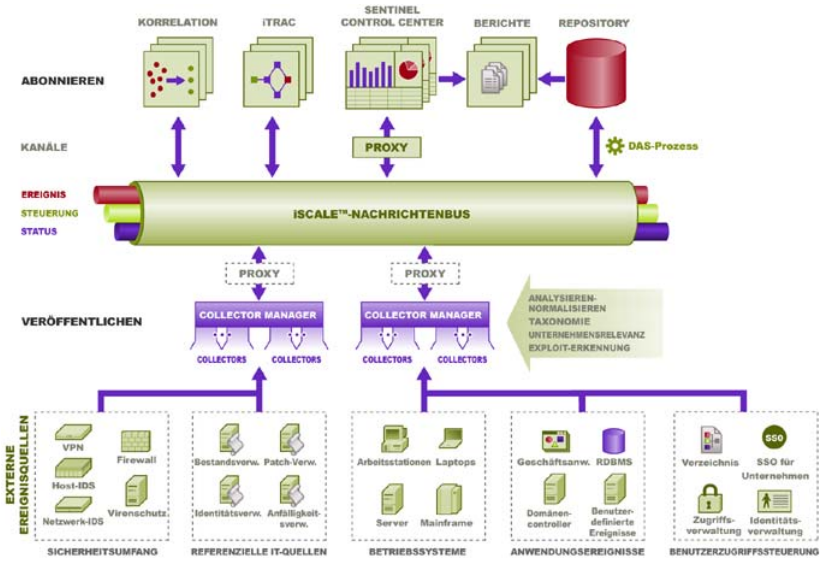
```
Restart the “Sentinel” service using the Windows Service Manager.
```

Kommunikationsschicht (iSCALE) 7

- Abschnitt 7.1, „SSL-Proxy und direkte Kommunikation“, auf Seite 96
- Abschnitt 7.2, „Ändern des Kommunikations-Verschlüsselungsschlüssels“, auf Seite 99
- Abschnitt 7.3, „Vergrößern der AES-Schlüsselstärke“, auf Seite 100

Die Kommunikationsschicht (iSCALE), die alle Komponenten der Architektur verbindet, ist eine verschlüsselte TCP/IP-Verbindung, die auf einem JMS-(Java Messaging Service-)Backbone erstellt wurde. Bei Sentinel 6 wurde ein optionaler SSL-Proxy hinzugefügt, um die Collector Manager- und Sentinel Control Center-Komponenten zu sichern, wenn diese außerhalb der Firewall installiert sind.

Abbildung 7-1 *Sentinel-Architektur*



Beim Installieren des Collector Managers sind zwei Kommunikationsoptionen verfügbar:

- **Direktes Verbinden mit dem Nachrichten-Bus (Standard):** Dies ist die einfachste und schnellste Option. Dafür muss der Collector Manager den Verschlüsselungsschlüssel des freigegebenen Nachrichten-Bus kennen, dies kann jedoch ein Sicherheitsrisiko darstellen, wenn der Collector Manager auf einem Computer ausgeführt wird, der Sicherheitsrisiken ausgesetzt ist (beispielsweise ein Computer in der DMZ). Mit dieser Option werden Kommunikationen mithilfe der AES-128-Bit-Verschlüsselung auf Grundlage der Daten in einer Datei mit Namen `.keystore` verschlüsselt.
- **Verbinden mit dem Nachrichten-Bus über den Proxy:** Mit dieser Option wird eine zusätzliche Sicherheitsschicht durch Konfigurieren des Collector Managers für das Verbinden über einen SSL-Proxyserver hinzugefügt. In diesem Fall wird die zertifikatsbasierte Authentifizierung und Verschlüsselung verwendet, sodass die Datei `.keystore` nicht auf dem Collector Manager-Computer gespeichert werden muss. Dies ist sinnvoll, wenn der Collector Manager in einer weniger sicheren Umgebung installiert ist.

Es kann beim Installieren des Collector Managers eine dieser Optionen ausgewählt werden. Das Sentinel Control Center verwendet standardmäßig den Proxy.

7.1 SSL-Proxy und direkte Kommunikation

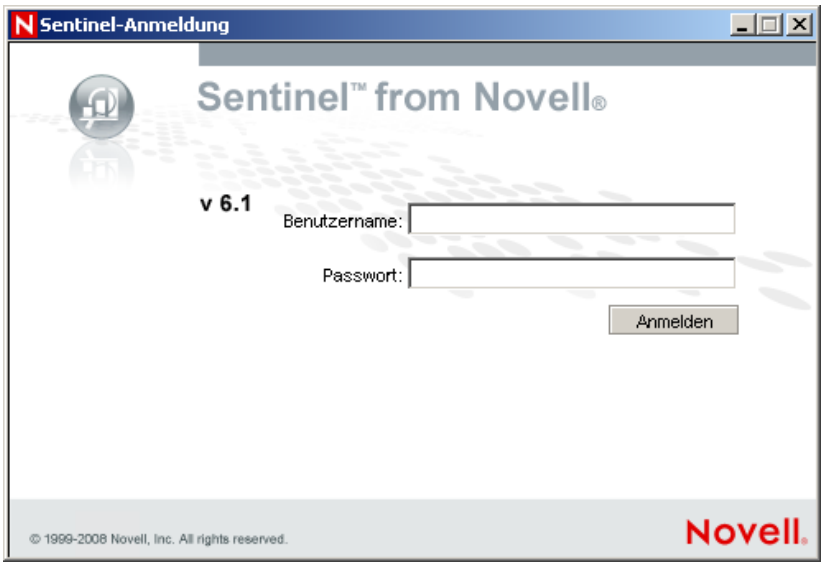
Die Sentinel-Komponenten, die den SSL-Proxy verwenden könnten, sind das Sentinel Control Center und der Collector Manager.

7.1.1 Sentinel Control Center

Das Sentinel Control Center verwendet standardmäßig den SSL-Proxy. Das Sentinel Control Center wird mit SSL über den `proxied_client`-Port verbunden. Dieser Port ist so eingerichtet, dass er nur die serverseitige SSL-Zertifikatsauthentifizierung verwendet. Die clientseitige Authentifizierung verwendet Benutzernamen und Passwort des Sentinel Control Center-Benutzers.

So melden Sie sich erstmalig beim Sentinel Control Center an:

1 Gehen Sie zu „Start“ > „Programme“ > „Sentinel“ und wählen Sie „Sentinel Control Center“ aus. Das Fenster „Sentinel-Anmeldung“ wird angezeigt.

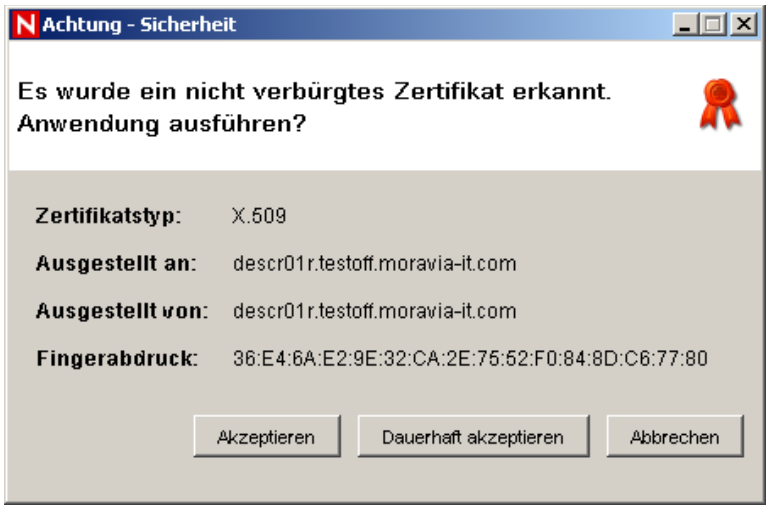


2 Geben Sie die Benutzerberechtigungen an, mit denen Sie sich beim Sentinel Control Center anmelden.

- Benutzername und Passwort bei Verwendung von SQL Server-Authentifizierung, ODER
- Domäne\Benutzername und Passwort bei Verwendung von Windows-Authentifizierung

3 Klicken Sie auf Anmelden.

4 Beim ersten Anmeldeversuch wird eine Warnmeldung wie unten angezeigt.



5 Wenn Sie „Akzeptieren“ auswählen, wird diese Meldung jedes Mal angezeigt, wenn Sie versuchen, Sentinel auf dem System zu öffnen Um dies zu vermeiden, können Sie „Dauerhaft akzeptieren“ auswählen.

So starten Sie das Sentinel Control Center unter Linux und Solaris:

1 Ändern Sie das Verzeichnis als Sentinel Administrator -Benutzer („esecadm“) in:
`$ESEC_HOME/bin`

2 Führen Sie den folgenden Befehl aus:
`control_center.sh`

3 Geben Sie Ihren Benutzernamen und Ihr Passwort an und klicken Sie auf „OK“.

4 Das Fenster „Zertifikat“ wird angezeigt. Klicken Sie auf „Akzeptieren“.

Die Sentinel Control Center-Benutzer müssen die oben genannte Prozedur wiederholen, um ein neues Zertifikat unter diesen Umständen zu akzeptieren:

- Der Sentinel-Kommunikationsserver wird neu installiert.
- Der Sentinel-Kommunikationsserver wird zu einem neuen Server verschoben.

7.1.2 Collector Manager

Der Collector Manager kann entweder im Proxymodus (unter Verwendung des SSL-Proxys) oder im direkten Modus (direktes Verbinden mit dem Nachrichten-Bus) installiert werden.

- Bei den Collector Managers, die leichter gefährdet sein können (beispielsweise bei einem Computer im DMZ), ist der SSL-Proxy die sicherere Kommunikationsmethode.
- Bei den Collector Managers in einer sichereren Umgebung oder in einer Umgebung, in der ein hoher Ereignisdurchsatz wichtig oder auf demselben Computer wie der Data Access Service (DAS) installiert ist, wird die direkte Kommunikation mit dem Nachrichten-Bus empfohlen.

Der Collector Manager wird mit SSL über den `proxied_trusted_client` verbunden. Um zu ermöglichen, dass der Collector Manager nach einem Neustart ohne menschliches Eingreifen neu gebootet wird, ist dieser Port so eingerichtet, dass sowohl die serverseitige als auch die clientseitige SSL-Zertifikatauthentifizierung verwendet wird. Eine verbürgte Beziehung wird zwischen dem

Proxy und Collector Manager (Zertifkataustausch) eingerichtet, wobei zukünftige Verbindungen die Zertifikate für die Authentifizierung verwenden. Diese verbürgte Beziehung wird automatisch während der Installation eingerichtet.

Die verbürgte Beziehung muss für jeden Collector Manager, der den SSL-Proxy verwendet, zurückgesetzt werden, wenn die folgenden Bedingungen zutreffen:

- Der Sentinel-Kommunikationsserver wird neu installiert.
- Der Sentinel-Kommunikationsserver wird zu einem neuen Server verschoben.

Diese Prozedur kann auch verwendet werden, um einen Collector Manager vom direkten Modus in den Proxymodus zu ändern.

So setzen Sie eine verbürgte Beziehung für einen Collector Manager zurück:

1. Melden Sie sich beim Collector Manager-Server als Sentinel-Administrator (standardmäßig „esecadm“) an.
2. Öffnen Sie die Datei `configuration.xml` in „$ESEC_HOME/config“ oder „%ESEC_HOME%\config“ in einem Texteditor.
3. Ändern Sie die Dienste „Collector_Manager“, „agentmanager_events“ und „Sentinel“ in der Datei `configuration.xml` so, dass die Strategie-ID„proxied_trusted_client“ verwendet wird. Hier ist ein Auszug aus einer Beispieldatei:

   ```
   <service name="Collector_Manager" plugins=""
   strategyid="proxied_trusted_client"/>
   <service name="agentmanager_events" plugins=""
   strategyid="proxied_trusted_client"/>
   <service name="Sentinel" plugins=""
   strategyid="proxied_trusted_client"/>
   ```

4. Speichern Sie die Datei und beenden Sie den Vorgang.
5. Führen Sie `%ESEC_HOME%\bin\register_trusted_client.bat` aus (oder unter UNIX die Datei `.sh`). Es wird eine Ausgabe ähnlich wie die folgende angezeigt:

   ```
   E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
   Please review the following server certificate:
   Type: X.509
   Issued To: foo.bar.net
   Issued By: foo.bar.net
   Fingerprint (MD5): A8:DF:BA:B2:F3:21:C9:27:28:48:13:B3:FE:F8:B4:AD
   Would you like to accept this certificate? [Y/N] (defaults to N): Y
   Please enter a Sentinel username and password that has permissions
   to register a trusted client.
   Username: esecadm
   Password:*********
   *Writing to keystore file: E:\Program
   Files\Novell\Sentinel6\config\.proxyClientKeystore
   ```

6. Starten Sie den Sentinel-Dienst auf dem Server neu, auf dem der Collector Manager gehostet wird.
7. Wiederholen Sie diese Schritte auf allen Collector Managers mithilfe der Proxykommunikation.

7.2 Ändern des Kommunikations-Verschlüsselungsschlüssels

Die Sentinel-Installation ermöglicht es dem Administrator, einen neuen, zufälligen Verschlüsselungsschlüssel zu generieren (gespeichert in der Datei `.keystore`) oder eine vorhandene Datei `.keystore` zu importieren. Bei jedem Ansatz muss die Datei `.keystore` auf jedem Computer, auf dem eine Sentinel-Serverkomponente installiert ist, identisch sein, damit die Kommunikation ordnungsgemäß funktioniert.

Hinweis: Die Datei `.keystore` ist auf dem Datenbankcomputer nicht erforderlich, wenn die Datenbank die einzige auf diesem Computer installierte Sentinel-Komponente ist. Sie ist außerdem nicht auf Computern erforderlich, auf denen nur das Sentinel Control Center, Collector Builder, Sentinel Data Manager oder der Collector Manager (mit einem Proxy) installiert ist.

Der Verschlüsselungsschlüssel kann nach der Installation mithilfe des Dienstprogramms `keymgr` geändert werden. Dieses Dienstprogramm generiert eine Datei mit einem zufällig generierten Verschlüsselungsschlüssel. Diese Datei muss auf jeden Computer kopiert werden, auf dem eine Sentinel-Serverkomponente installiert ist.

So ändern Sie den Verschlüsselungsschlüssel für die direkte Kommunikation:

1. Melden Sie sich bei UNIX als Sentinel-Administrator an (standardmäßig „esecadm“). Melden Sie sich unter Windows als Benutzer mit Administratorrechten an.
2. Navigation:

   Bei UNIX:

   `$ESEC_HOME/lib`

   Für Windows:

   `%ESEC_HOME%\lib`
3. Führen Sie den folgenden Befehl aus:

   Unter UNIX:

   ```
   keymgr.sh --keyalgo AES --keysize 128 --keystore <output filename,
   usually .keystore>
   ```

   Unter Windows:

   ```
   keymgr.bat --keyalgo AES --keysize 128 --keystore <output filename,
   usually .keystore>
   ```
4. Kopieren Sie die Datei `.keystore` auf jeden Computer, auf dem eine Sentinel-Serverkomponente installiert ist (außer es wird Proxykommunikation verwendet). Die Datei sollte an folgenden Speicherort kopiert werden:

   Bei UNIX:

   `$ESEC_HOME/config`

   Für Windows:

   `%ESEC_HOME%\config`

Hinweis: Wenn Sie den Advisor im direkten Downloadmodus verwenden, müssen Sie das in den Konfigurationsdateien des Advisors gespeicherte Advisor-Passwort aktualisieren. Dieses Passwort wurde mithilfe der Informationen in der Datei `.keystore` verschlüsselt und muss unter Verwendung des neuen `.keystore`-Werts neu erstellt werden. Folgen Sie zum Aktualisieren des Passworts den Anweisungen in Kapitel 4, „Advisor-Konfiguration“, auf Seite 65.

7.3 Vergrößern der AES-Schlüsselstärke

Sentinel verwendet AES-Verschlüsselung für die Kommunikation über Sonic und Verschlüsselungspasswörter, die in Konfigurationsdateien gespeichert sind und über Sonic gesendet werden. Sentinel verwendet aufgrund von bestimmten wichtigen Beschränkungen standardmäßig den AES-128-Bit-Verschlüsselungsalgorithmus . Wenn diese wichtigen Beschränkungen nicht auf Sie zutreffen, können Sie Sentinel so konfigurieren, dass ein stärkerer AES-256-Bit-Algorithmus verwendet wird.

Hinweis: Es wird dringend empfohlen, den Abschnitt „Understanding the Export/Import Issues“ (Wissenswertes zu Export-/Importproblemen) der Java-Datei `Readme.txt` lesen, bevor Sie die 256-Bit-Verschlüsselung aktivieren.

So konfigurieren Sie die AES-256-Bit-Verschlüsselung:

1. Laden Sie die „Unlimited Encryption“-Richtlinien von Sun unter „http://java.sun.com/javase/downloads/index_jdk5.jsp“ herunter (http://java.sun.com/javase/downloads/index_jdk5.jsp). Laden Sie im Bereich „Other Downloads“ (andere Downloads) „Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0“ herunter.
2. Wenden Sie die oben genannte Richtliniendatei auf alle JREs an, die Prozesse ausführen, die direkt mit Sonic verbunden werden (DAS, Correlation Engine, Communication Server, Collector Manager, wenn diese im Modus „Direct to Sonic“ verwendet werden). Informationen zum Anwenden der Richtliniendateien finden Sie in der Datei `Readme.txt`, die in der Richtlinie vorhanden ist, die Sie heruntergeladen haben.
3. Verwenden Sie das Dienstprogramm „keymgr“, um eine 256-Bit-`AES .keystore`-Datei mithilfe der Anweisungen im Abschnitt Abschnitt 7.2, „Ändern des Kommunikations-Verschlüsselungsschlüssels“, auf Seite 99 zu generieren.
4. Kopieren Die diese Datei `.keystore` auf alle Computer in Schritt 2 und platzieren Sie sie im Verzeichnis „$ESEC_HOME/config“ oder „%ESEC_HOME%\config“.

Hinweis: Wenn Sie den Advisor im direkten Downloadmodus verwenden, müssen Sie das in den Konfigurationsdateien des Advisors gespeicherte Advisor-Passwort aktualisieren. Dieses Passwort wurde mithilfe der Informationen in der Datei `.keystore` verschlüsselt und muss unter Verwendung des neuen `.keystore`-Werts neu erstellt werden. Weitere Informationen zum Aktualisieren eines Passworts finden Sie unter “Zertifikatsverwaltung für DAS_Proxy” im *Referenzhandbuch*.

Crystal Reports für Windows

8

- Abschnitt 8.1, „Überblick“, auf Seite 102
- Abschnitt 8.2, „Systemanforderungen“, auf Seite 103
- Abschnitt 8.3, „Konfigurationsanforderungen“, auf Seite 103
- Abschnitt 8.4, „Bekannte Probleme“, auf Seite 105
- Abschnitt 8.5, „Verwenden von Crystal Reports“, auf Seite 105
- Abschnitt 8.6, „Installationsüberblick“, auf Seite 105
- Abschnitt 8.7, „Installation“, auf Seite 106
- Abschnitt 8.8, „Konfiguration für alle Authentifizierungen und Konfigurationen“, auf Seite 120
- Abschnitt 8.9, „Veröffentlichen Sie Crystal Reports-Schablonen“, auf Seite 121
- Abschnitt 8.10, „Auf Hochleistung ausgerichtete Konfigurationen für Crystal“, auf Seite 128

Crystal Reports Server™ (von Business Objects) ist das Berichterstellungswerkzeug, das mit Sentinel verwendet wird. In diesem Abschnitt wird die Installationskonfiguration von Crystal Reports Server für Sentinel erörtert. Weitere Informationen zu unterstützten Plattformen für Crystal Reports Server in einer Sentinel-Umgebung finden Sie unter Kapitel 2, „Systemanforderungen“, auf Seite 21.

Unter Windows wurde Sentinel mit Crystal Reports Server XI R2 SP3 getestet. Weitere Informationen zu Crystal Reports Server XI Release 2 Service Packs erhalten Sie unter https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads). Suchen Sie dort nach der gewünschten Version und Plattform.

In diesem Abschnitt wird das Ausführen von Crystal Reports Server unter Windows erläutert. Weitere Informationen zum Ausführen von Crystal Reports Server unter Linux/Solaris finden Sie unter .

So installieren Sie Crystal Reports Server:

1. Installation von Microsoft IIS und ASP.NET
2. Installation von Microsoft SQL (je nach Konfiguration als Windows-Authentifizierung oder SQL Server-Authentifizierung)
3. Nur für chinesische (traditionell und einfach) und japanische Benutzer: Installation von asiatischen Schriftarten (beispielsweise Arial Unicode MS) zum Anzeigen von Berichten in diesen Sprachen.
4. Installation von Crystal Reports Server
   - Konfiguration von Open Database Connectivity (ODBC) für SQL-Authentifizierung

     oder
   - Installation und Konfiguration der Oracle 9i-Client-Software
5. Konfiguration von `inetmgr`
6. Anwendung von Crystal Reports

7 Veröffentlichen (Importieren) von Crystal Reports-Berichten

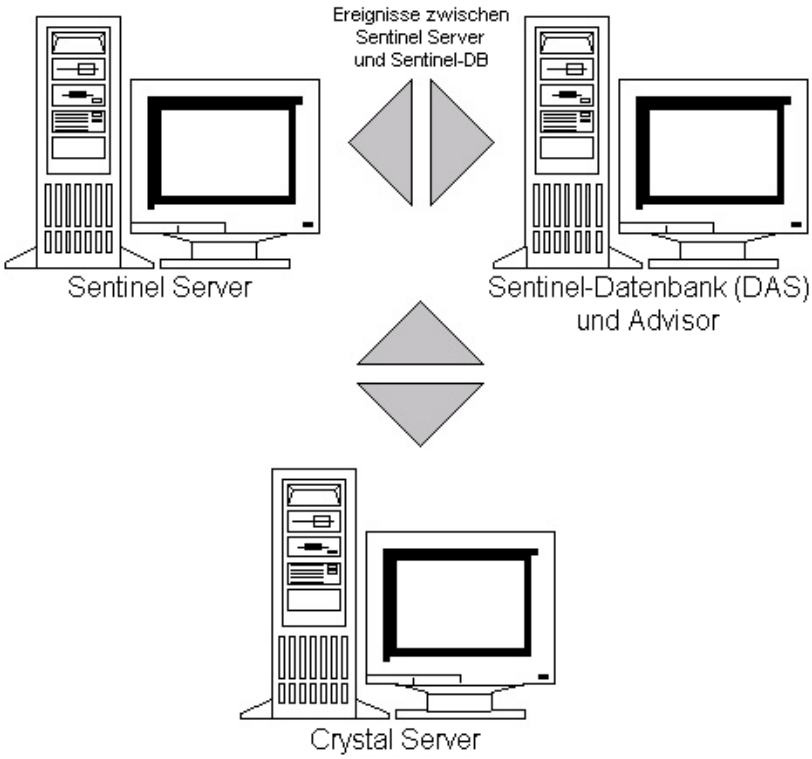
8 Festlegen eines Kontos für einen benannten Benutzer

9 Testen der Konnektivität zum Webserver

10 Erhöhen der Datensatzbeschränkung zum Aktualisieren von Crystal Reports Server-Berichten (empfohlen)

11 Konfigurieren Sie das Sentinel Control Center für die Integration mit Crystal Reports Server.

Hinweis: Sie müssen die Komponenten in der oben angegebenen Reihenfolge installieren.



8.1 Überblick

Crystal Reports Server benötigt eine Datenbank zum Speichern von Informationen über das System und dessen Benutzer. Diese Datenbank ist als Central Management Server-(CMS-)Datenbank bekannt. Der CMS ist ein Server, der Informationen über das Crystal Reports Server-System speichert. Nach Bedarf können weitere Komponenten von Crystal Reports Server Zugriff auf diese Informationen erlangen.

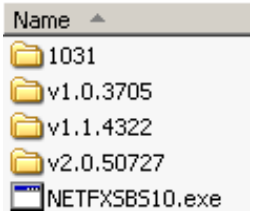
Es ist erforderlich, die CMS-Datenbank für eine Crystal-Installation unter Windows über einer lokalen Microsoft SQL Server-Datenbank zu installieren. Das Installationsprogramm von Crystal Reports Server ermöglicht zwar das Einrichten der CMS-Datenbank über der MSDE-Datenbank, diese Konfiguration wurde jedoch für Sentinel weder getestet noch wird sie unterstützt.

8.2 Systemanforderungen

Windows® 2003 Server mit SP1 mit einer NTFS-formatierten Partition und installiertem IIS (Microsoft Internet Information Service) und .ASP.NET. Sentinel unterstützt Crystal X2 auf Windows® 2000 Server nicht.

.NET Framework 1.1 oder 2.0 (Standardmäßig auf Windows 2003 installiert) Wechseln Sie zu „ %SystemRoot%\Microsoft.NET\Framework“, um zu bestimmen, welche Version von .NET Framework auf dem Computer vorhanden ist. Der Ordner mit dem höchsten numerischen Wert sollte maximal die Nummer v.1.1.xxxx aufweisen. Beispiel:

Abbildung 8-1 *.NET Framework-Version*



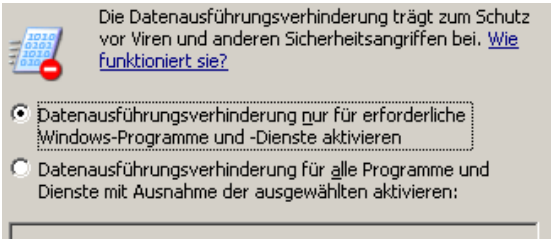
Weitere Informationen zu unterstützten Plattformen für Crystal Reports Server in einer Sentinel-Umgebung erhalten Sie unter Kapitel 2, „Systemanforderungen“, auf Seite 21.

8.3 Konfigurationsanforderungen

1. Stellen Sie sicher, dass das Konto, das zum Installieren von Crystal Reports Server verwendet wurde, über lokale Administratorrechte verfügt.
2. Stellen Sie die Datenausführungsverhinderung (DEP, Data Execution Prevention) so ein, dass sie nur für die ausgewählten Programme und Services ausgeführt wird. Dies ist insbesondere hilfreich zur Vermeidung des folgenden Fehlers: „Error 1920. Service ‘Crystal Report Cache Server’ on Windows 2003“.

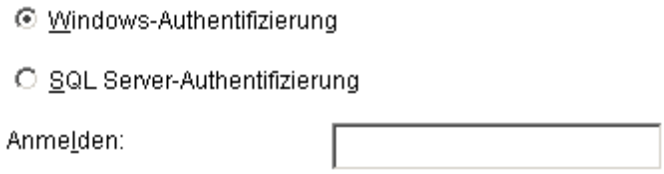
   Der Zugriff auf die Datenausführungsverhinderung erfolgt über Systemsteuerung > System > Registerkarte „Erweitert“ > Leistungseinstellungen > Datenausführungsverhinderung.

   Wählen Sie die Datenausführungsverhinderung nur für wichtige Windows-Programme und -Services aus.


Die Datenausführungsverhinderung trägt zum Schutz vor Viren und anderen Sicherheitsangriffen bei. Wie funktioniert sie?
Datenausführungsverhinderung nur für erforderliche Windows-Programme und -Dienste aktivieren
Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten aktivieren:

3. Voraussetzung für die Installation und Konfiguration von Crystal Reports Server ist, dass der Sentinel-Server und die -Datenbank bereits installiert wurden. Sie müssen wissen, welcher Authentifizierungsmodus für den Sentinel Report-Benutzer ausgewählt wurde. Dieser Benutzer heißt „esecrpt“, falls Sie die lokale Datenbankauthentifizierung verwenden. Bei Verwendung

der Windows-Authentifizierung können Sie einen beliebigen Namen vergeben. Der Authentifizierungsmodus wurde während des Sentinel-Installationsvorgangs in einem Fenster ähnlich dem folgenden eingestellt.



Hinweis: Sie können das esecrpt-Passwort explizit in Windows setzen.

4 Die Videoauflösung sollte auf 1024 x 768 oder höher festgelegt werden.

5 Installation von Microsoft Internet Information Server (IIS) und ASP.NET

Hinweis: Sentinel unterstützt das Verwenden von MSDE als Crystal CMS-Datenbank nicht. Installieren Sie Microsoft SQL Server 2005 vor der Installation von Crystal Reports Server XI R2.

8.3.1 Installation von Microsoft Internet Information Server (IIS) und ASP.NET

Zum Hinzufügen dieser Windows-Komponenten benötigen Sie eventuell die Installations-CD von Windows 2003 Server.

So installieren Sie IIS und ASP.NET:

1 Wechseln Sie zu „Systemsteuerung“ > „Software“.

2 Klicken Sie im linken Fensterbereich auf Windows-Komponenten hinzufügen/entfernen.

3 Wählen Sie Anwendungsserver aus.

4 Klicken Sie auf "Details".

5 Wählen Sie ASP.NET und Internet Information Services (IIS) aus.

6 Klicken Sie auf „OK“.

7 Klicken Sie anschließend auf "Weiter". Möglicherweise werden Sie aufgefordert, die Windows-Installations-CD einzulegen.

8 Klicken Sie auf Fertig stellen.

8.4 Bekannte Probleme

- **Installieren von Crystal Reports:** Novell stellt zwei Crystal-Schlüssel aus, einen für Crystal Reports Server und den anderen für Crystal Reports Developer (zum Ändern oder Erstellen von neuen Berichten). Achten Sie darauf, bei der Installation von Crystal Reports Server den zugehörigen Schlüssel zu verwenden.
- **Deinstallieren von Crystal Reports:** Sollten Sie Crystal Reports Server deinstallieren müssen, können Sie die Registrierungsschlüssel mithilfe eines manuellen Deinstallationsverfahrens bereinigen. Dies ist besonders nützlich, wenn Ihre Installation beschädigt wird. Wechseln Sie zu der folgenden Business Objects-Website, um Prozeduren zum manuellen Deinstallieren von Crystal Reports Server abzurufen: http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Hinweis: Die oben stehende URL war zum Veröffentlichungszeitpunkt dieses Dokuments korrekt.

8.5 Verwenden von Crystal Reports

Weitere Informationen zum Verwenden von Crystal Reports Server für Sentinel Reporting finden Sie in der Crystal Reports Server-Dokumentation (http://support.businessobjects.com/documentation/product_guides/default.asp) und im *Sentinel-Benutzerhandbuch*.

8.6 Installationsüberblick

8.6.1 Installationsüberblick für Crystal mit SQL Server 2005

Dies sind die wichtigsten Schritte für die Installation von Crystal Reports Server mit einer Microsoft SQL Server 2005 Sentinel-Datenbank unter Verwendung der Windows-Authentifizierung oder der SQL-Authentifizierung. Die einzelnen Schritte werden im Rest dieses Abschnitts ausführlicher beschrieben.

1. Installation von Crystal Reports Server XI R2
   - Siehe Abschnitt 8.7.1, „Installation von Crystal Reports Server für MS SQL Server 2005 mit Windows-Authentifizierung“, auf Seite 106, wenn Sie die Windows-Authentifizierung für den Sentinel Report-Benutzer beim Installieren von Sentinel ausgewählt haben.
   - Siehe Abschnitt 8.7.2, „Installation von Crystal Reports Server für Microsoft SQL Server 2005 mit SQL-Authentifizierung“, auf Seite 112, wenn Sie die SQL-Authentifizierung für den Sentinel Report-Benutzer beim Installieren von Sentinel ausgewählt haben.
2. Konfigurieren von Open Database Connectivity (ODBC)
3. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
4. Anwenden von Crystal Reports
5. Veröffentlichen von Berichten
6. Festlegen des Kontos für einen benannten Benutzer

7 Erstellen einer Crystal-Webseite (Abschnitt 8.9.5, „Konfigurieren von Berichtsberechtigungen“, auf Seite 125)

8 Konfigurieren von Sentinel für Crystal Reports Server

Hinweis: Diese Schritte müssen in der richtigen Reihenfolge ausgeführt werden.

8.6.2 Installationsüberblick für Crystal mit Oracle

Dies sind die wichtigsten Schritte für die Installation von Crystal Reports Server mit einer Oracle Sentinel-Datenbank. Die einzelnen Schritte werden im Rest dieses Abschnitts ausführlicher beschrieben.

Führen Sie zur ordnungsgemäßen Installation von Crystal Reports folgendes Verfahren in der angegebenen Reihenfolge durch.

1 Installieren von Oracle Client und Konfigurieren des systemeigenen Oracle-Treibers

2 Nur für chinesische (traditionell und einfach) und japanische Benutzer: Installation von asiatischen Schriftarten (beispielsweise Arial Unicode MS) zum Anzeigen von Berichten in diesen Sprachen.

3 Installieren von Crystal Reports Server XI R2. Weitere Informationen finden Sie unter Abschnitt 8.7.3, „Installation von Crystal Reports Server für Oracle“, auf Seite 116.

4 Zuordnen von Crystal Reports zur Verwendung mit Sentinel

5 Importieren Sie Crystal Report-Schablonen.

6 Erstellen einer Crystal-Webseite (Abschnitt 8.9.5, „Konfigurieren von Berichtsberechtigungen“, auf Seite 125)

7 Konfigurieren von Sentinel für Crystal Reports Server

Hinweis: Diese Schritte müssen in der richtigen Reihenfolge ausgeführt werden.

8.7 Installation

In diesem Abschnitt wird die Installation von Crystal Reports Server für folgende Elemente beschrieben:

- Abschnitt 8.7.1, „Installation von Crystal Reports Server für MS SQL Server 2005 mit Windows-Authentifizierung“, auf Seite 106
- Abschnitt 8.7.2, „Installation von Crystal Reports Server für Microsoft SQL Server 2005 mit SQL-Authentifizierung“, auf Seite 112
- Abschnitt 8.7.3, „Installation von Crystal Reports Server für Oracle“, auf Seite 116

8.7.1 Installation von Crystal Reports Server für MS SQL Server 2005 mit Windows-Authentifizierung

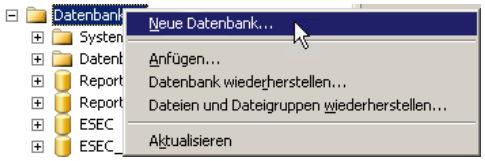
So installieren Sie Crystal Reports Server mit Windows-Authentifizierung:

1 Installieren Sie Microsoft SQL Server 2005 im gemischten Modus.

2 Starten Sie Microsoft SQL Server Management Studio.

3 Erweitern Sie „Databases“ (Datenbanken) im Navigationsbereich

Heben Sie „Database“ (Datenbank) hervor, klicken Sie mit der rechten Maustaste darauf und wählen Sie „New Database“ (Neue Datenbank) aus, um die Crystal CMS-Datenbank zu erstellen.



4 Geben Sie unter dem Feld für den Datenbanknamen BOE115 an und klicken Sie auf „OK“.

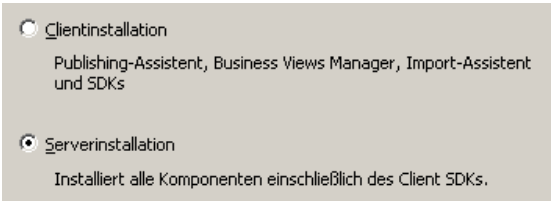
5 Beenden Sie Microsoft SQL Server Management Studio.

6 Geben Sie die Crystal Reports XI R2 Server-CD in das CD-ROM-Laufwerk ein.

7 Wenn auf Ihrem Computer „Autoplay“ deaktiviert ist, führen Sie die Datei `setup.exe` aus.

8 Wählen Sie die Crystal Reports-Setupsprache aus.

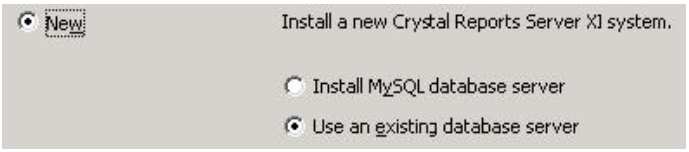
9 Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option „Perform Server Installation“ (Serverinstallation durchführen) aus.


Clientinstallation
Publishing-Assistent, Business Views Manager, Import-Assistent und SDKs
Serverinstallation
Installiert alle Komponenten einschließlich des Client SDKs.

10 Geben Sie den Crystal-Lizenzschlüssel an (von Novell Kunden-Center (https://secure-www.novell.com/center/regadmin)).

11 Legen Sie einen Zielordner fest.

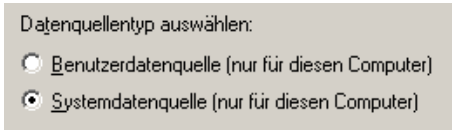
12 Wählen Sie als Installationstyp „Use an existing database server“ (Vorhandenen Datenbankserver verwenden) aus.



13 Klicken Sie im Bereich „CMS Database“ (CMS-Datenbank) auf „Browse“ (Durchsuchen).

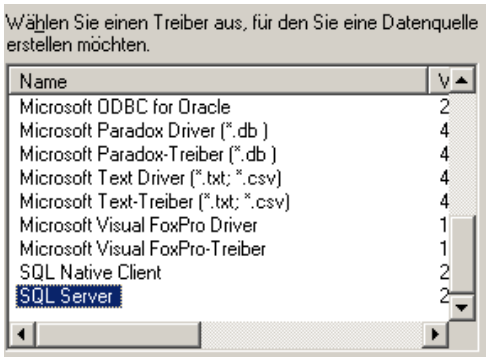
14 Klicken Sie auf die Registerkarte „Machine Data Source“ (Computerdatenquelle). Klicken Sie auf "Neu".

15 Wählen Sie „System Data Source“ (Systemdatenquelle) aus.

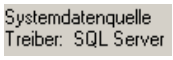

Datenquellentyp auswählen:
Benutzerdatenquelle (nur für diesen Computer)
Systemdatenquelle (nur für diesen Computer)

Klicken Sie anschließend auf "Weiter".

16 Blättern Sie nach unten, wählen Sie SQL Server und klicken Sie auf Next (Weiter).


Wählen Sie einen Treiber aus, für den Sie eine Datenquelle erstellen möchten.
Name
V
Microsoft ODBC for Oracle 2
Microsoft Paradox Driver (*.db) 4
Microsoft Paradox-Treiber (*.db) 4
Microsoft Text Driver (*.txt; *.csv) 4
Microsoft Text-Treiber (*.txt; *.csv) 4
Microsoft Visual FoxPro Driver 1
Microsoft Visual FoxPro-Treiber 1
SQL Native Client 2
SQL Server 2

17 Eine neue Quelle wird angezeigt. Klicken Sie auf „Finish“ (Beenden).

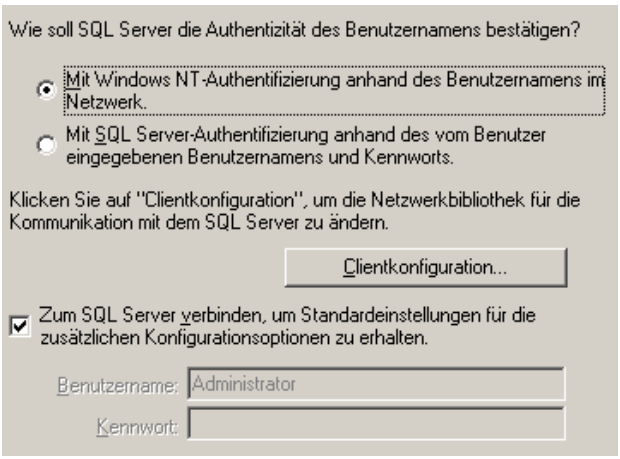


18 Geben Sie im Fenster „New Data Source to SQL Server“ (Neue Datenquelle für SQL Server) Folgendes an:

- Name Ihrer Datenquelle (z. B. „BOE_XI“)
- Beschreibung (optional)
- Klicken Sie zur Auswahl des Servers auf den nach unten weisenden Pfeil und wählen Sie (local) (lokal) aus.

Klicken Sie anschließend auf "Weiter".

19 Wenn nicht bereits geschehen, wählen Sie „With Windows NT“ (Mit Windows NT) aus.


Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.
Klicken Sie auf "Clientkonfiguration", um die Netzwerkbibliothek für die Kommunikation mit dem SQL Server zu ändern.
Clientkonfiguration...
Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten.
Benutzername:
Administrator
Kennwort:

Hinweis: Die Anmelde-ID (abgeblendet - nicht verfügbar) ist Ihr Windows-Anmeldename.

---

20 Aktivieren Sie das Kontrollkästchen „Change default database to“ (Standarddatenbank ändern in:). Ändern Sie Ihre Standarddatenbank in „BOE115“. Klicken Sie anschließend auf "Weiter".

21 Klicken Sie im Fenster „Create a New Data Source to SQL Server“ (Neue Datenquelle für SQL Server erstellen) auf „Finish“ (Fertig stellen).

22 Klicken Sie auf „Test Data Source“ (Datenquelle testen) und testen Sie die Datenquelle. Nachdem Sie die Datenquelle getestet haben, klicken Sie auf „OK“.

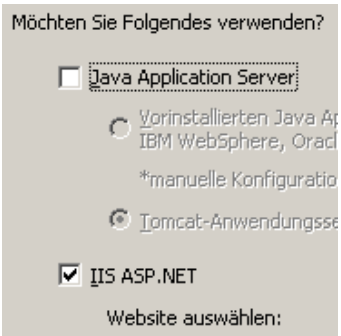
23 Markieren Sie im Fenster „Select Data Source“ (Datenquelle auswählen) die Option „BOE115“ und klicken Sie so lange auf „OK“, bis das Dialogfeld „SQL Server Login“ (SQL Server-Anmeldung) angezeigt wird. Vergewissern Sie sich, dass Use Trusted Connection (Vertrauenswürdige Verbindung verwenden) ausgewählt ist. Klicken Sie auf "OK".

Hinweis: Die „Login ID“ (Anmelde-ID) (abgeblendet – nicht verfügbar) ist Ihr Windows-Anmeldename.

---

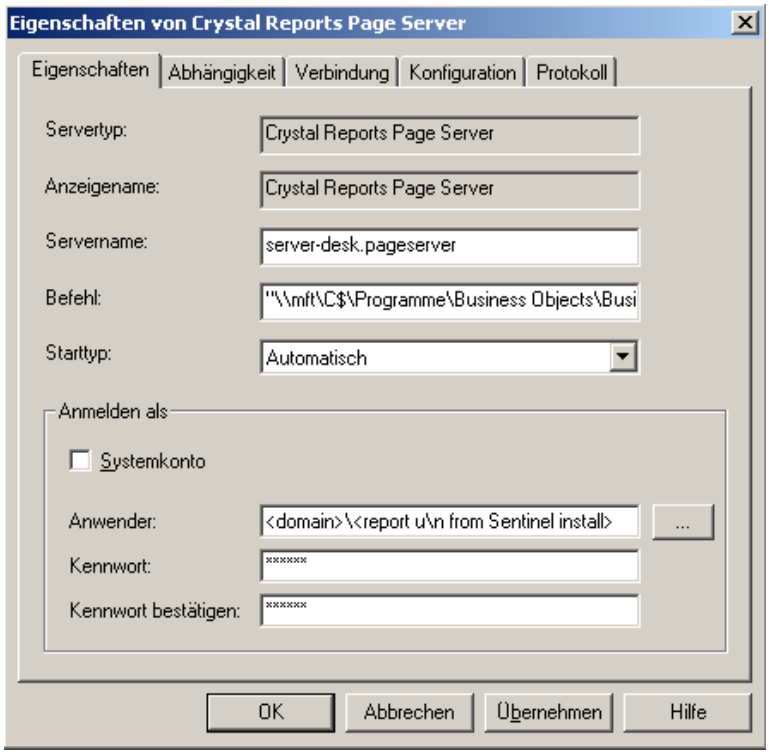
24 Wählen Sie im Fenster „Web Component Adapter Type“ (Adaptertyp der Webkomponente) die Option IIS ASP.NET aus.

Hinweis: Wenn Sie IIS und ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert haben, ist IIS/ASP.NET abgeblendet (nicht verfügbar).



25 Nach der Installation müssen Sie das Anmeldekonto für Crystal Reports Page Server und Crystal Reports Job Server in das Domänenkonto des Sentinel Report-Benutzers ändern.

- Klicken Sie auf Start > Programme > BusinessObjects > Crystal Reports Server > Central Configuration Manager.
- Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und wählen Sie „Stop“ (Stopp).
- Klicken Sie mit der rechten Maustaste erneut auf „Crystal Reports Page Server“ und wählen Sie „Properties“ (Eigenschaften).
- Deaktivieren Sie die Option „Log On As System Account“ (Als Systemkonto anmelden) und geben Sie den Benutzernamen und das Passwort der Domäne des Sentinel Report-Benutzers ein, die während der Installation von Sentinel für den Sentinel Report-Benutzer verwendet wurden. Klicken Sie auf "OK".



26 Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und dann zum Starten erneut mit der rechten Maustaste.

Konfiguration von Open Database Connectivity (ODBC) für Windows-Authentifizierung

Hiermit wird ein Open Database Connectivity-(ODBC-)Datenquellenname eingerichtet, damit Crystal Reports Server über die Windows-Authentifizierung die Verbindung mit der Sentinel-Datenbank herstellen kann (unter Windows und SQL Server). Diese Schritte müssen auf dem Computer durchgeführt werden, auf dem Crystal Reports Server installiert ist.

So richten Sie eine ODBC-Datenquelle für die Windows-Authentifizierung ein:

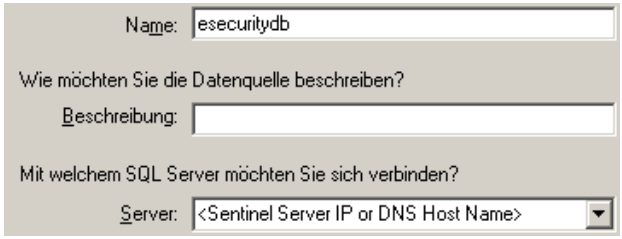
1 Wechseln Sie zu Windows-Systemsteuerung > Verwaltung > Datenquellen (ODBC).

2 Klicken Sie auf die Registerkarte „System-DSN“ und dann auf „Hinzufügen“.

3 Wählen Sie SQL Server. Klicken Sie auf Fertig stellen.

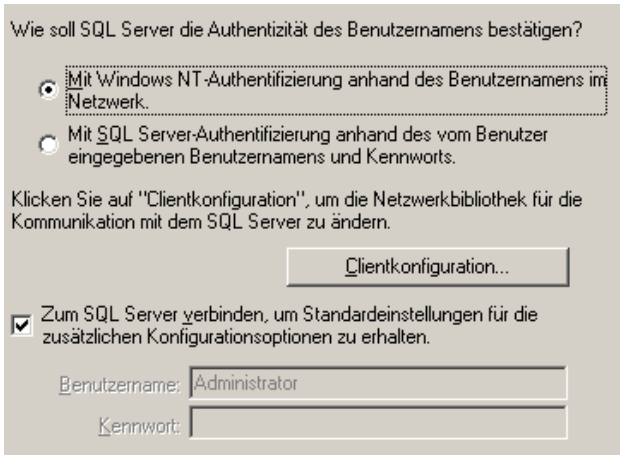
4 Daraufhin wird ein Fenster angezeigt, in dem Sie zur Eingabe von Informationen zur Treiberkonfiguration aufgefordert werden.

- Name der Datenquelle, geben Sie „esecuritydb“ ein
- Feld „Description“ (Beschreibung) (optional); geben Sie eine Beschreibung ein
- Feld „Server“; geben Sie Ihren Hostnamen bzw. die IP-Adresse Ihrer Instanz von Sentinel Server ein



5 Klicken Sie anschließend auf "Weiter".

Wählen Sie im nächsten Febster die Option für die Windows-Authentifizierung.


Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.
Klicken Sie auf "Clientkonfiguration", um die Netzwerkbibliothek für die Kommunikation mit dem SQL Server zu ändern.
Clientkonfiguration...
Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten.
Benutzername: Administrator
Kennwort:

Hinweis: Die „Login ID“ (Anmelde-ID) (abgeblendet – nicht verfügbar) ist Ihr Windows-Anmeldename.

---

6 Gehen Sie im nächsten Fenster wie folgt vor:

- Ändern Sie die Sentinel-Datenbank (Standardname: „ESEC“)
- Behalten Sie alle Standardeinstellungen bei.

Klicken Sie anschließend auf "Weiter".

7 Klicken Sie auf Fertig stellen.

8 Klicken Sie auf „Test Data Source“ (Datenquelle testen). Daraufhin wird eine Verbindung hergestellt. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

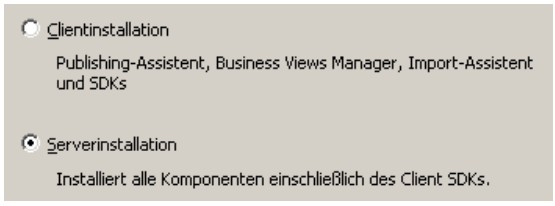
8.7.2 Installation von Crystal Reports Server für Microsoft SQL Server 2005 mit SQL-Authentifizierung

So installieren Sie Crystal Reports Server mit SQL-Authentifizierung:

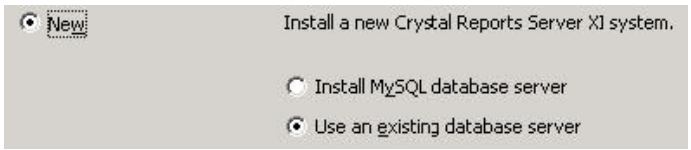
1. Installieren Sie Microsoft SQL Server 2005.
2. Rufen Sie Microsoft SQL Server Management Studio auf.
3. Erweitern Sie „Databases“ (Datenbanken) im Navigationsbereich

   Heben Sie „Database“ (Datenbank) hervor, klicken Sie mit der rechten Maustaste darauf und wählen Sie „New Database“ (Neue Datenbank) aus, um die Crystal CMS-Datenbank zu erstellen.

4. Geben Sie unter dem Feld für den Datenbanknamen BOE115 an und klicken Sie auf „OK“.
5. Beenden Sie Microsoft SQL Server Management Studio.
6. Legen Sie die Crystal Reports Server XI R2-CD in das CD-ROM-Laufwerk ein.
7. Wenn auf Ihrem Computer Autoplay deaktiviert ist, führen Sie die Datei `setup.exe` aus.
8. Wählen Sie die Crystal Reports-Setupsprache aus.
9. Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option „Perform Server Installation“ (Serverinstallation durchführen) aus.


Clientinstallation
Publishing-Assistent, Business Views Manager, Import-Assistent und SDKs
Serverinstallation
Installiert alle Komponenten einschließlich des Client SDKs.

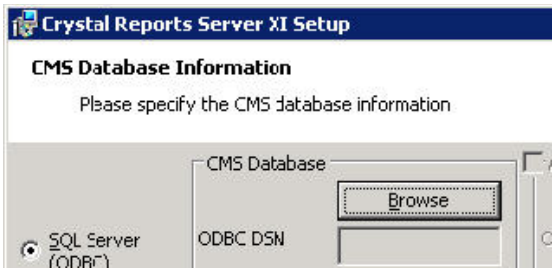
10. Geben Sie den Crystal-Lizenzschlüssel an (von Novell Kunden-Center (https://secure-www.novell.com/center/regadmin)).
11. Legen Sie einen Zielordner fest.
12. Wählen Sie als Installationstyp „Use an existing database server“ (Vorhandenen Datenbankserver verwenden) aus.



Hinweis: Crystal Reports Server und Microsoft SQL Server müssen sich auf demselben Computer befinden.

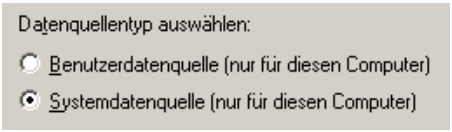
---

13 Klicken Sie im Bereich für die CMS-Datenbank auf „Browse“ (Durchsuchen).



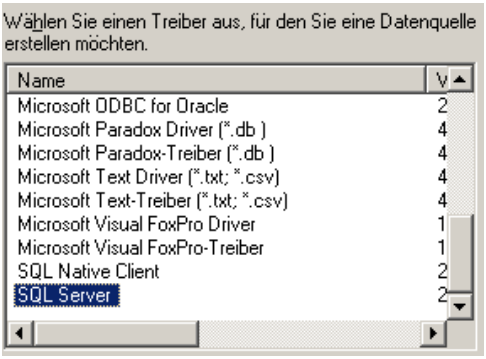
14 Klicken Sie auf die Registerkarte „Machine Data Source“ (Computerdatenquelle) und dann auf „New“ (Neu).

Wählen Sie „System Data Source“ (Systemdatenquelle) aus.


Datenquellentyp auswählen:
Benutzerdatenquelle (nur für diesen Computer)
Systemdatenquelle (nur für diesen Computer)

Klicken Sie anschließend auf "Weiter".

Blättern Sie nach unten, wählen Sie SQL Server und klicken Sie auf Next (Weiter).

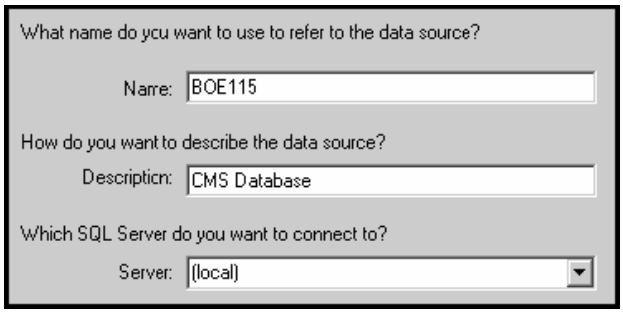

Wählen Sie einen Treiber aus, für den Sie eine Datenquelle erstellen möchten.
Name
Microsoft ODBC for Oracle
Microsoft Paradox Driver (*.db)
Microsoft Paradox-Treiber (*.db)
Microsoft Text Driver (*.txt; *.csv)
Microsoft Text-Treiber (*.txt; *.csv)
Microsoft Visual FoxPro Driver
Microsoft Visual FoxPro-Treiber
SQL Native Client
SQL Server

Eine neue Quelle wird angezeigt. Klicken Sie auf „Finish“ (Beenden).

15 Klicken Sie mit der rechten Maustaste auf „Databases“ (Datenbanken) und wählen Sie „Create New Database“ (Neue Datenbank erstellen) (BOE115).

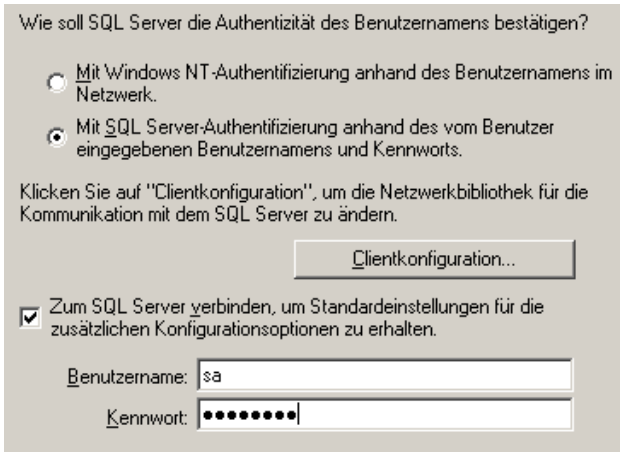
16 Geben Sie im Fenster „New Data Source to SQL Server“ (Neue Datenquelle für SQL Server) Folgendes ein:

- Name Ihrer Datenquelle (z. B. BOE115)
- Beschreibung (optional)
- Klicken Sie zur Auswahl des Servers auf den nach unten weisenden Pfeil und wählen Sie (local) (lokal) aus.


What name do ycu want to use to refer to the data source?
Name: BOE115
How do you want to describe the data source?
Descripticn: CMS Database
Which SQL Server do you want to connect to?
Server: (local)

Klicken Sie anschließend auf "Weiter".

17 Wählen Sie „With SQL Server Authentication“ (Mit SQL Server-Authentifizierung), geben Sie den „sa“ sowie das Passwort für den „sa“ an. Klicken Sie anschließend auf "Weiter".


Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.
Klicken Sie auf "Clientkonfiguration", um die Netzwerkbibliothek für die Kommunikation mit dem SQL Server zu ändern.
Clientkonfiguration...
Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten.
Benutzername: sa
Kennwort: ••••••••

Aktivieren Sie das Kontrollkästchen Change the default database to: (Standarddatenbank ändern in:). Ändern Sie Ihre Standarddatenbank in „BOE115“. Klicken Sie anschließend auf "Weiter".

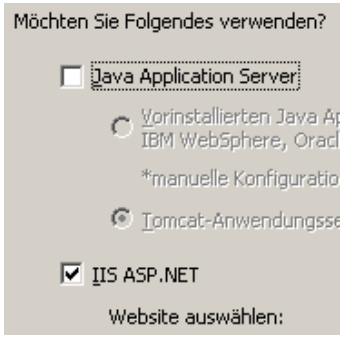
18 Klicken Sie im Fenster „Create a New Data Source to SQL Server“ (Neue Datenquelle für SQL Server erstellen) auf „Finish“ (Fertig stellen).

19 Klicken Sie auf „Test Data Source“ (Datenquelle testen). Klicken Sie auf "OK".

Markieren Sie im Fenster „Select Data Source“ (Datenquelle auswählen) die Option „BOE115“ und klicken Sie so lange auf „OK“, bis das Dialogfeld „SQL Server Login“ (SQL Server-Anmeldung) angezeigt wird. Vergewissern Sie sich, dass „Use Trusted Connection“ (Vertrauenswürdige Verbindung verwenden) NICHT ausgewählt ist. Klicken Sie auf OK. Klicken Sie anschließend auf "Weiter".

20 Wählen Sie im Fenster „Web Component Adapter Type“ (Adaptertyp der Webkomponente) die Option IIS ASP.NET aus.

Hinweis: Wenn Sie IIS und ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert haben, ist IIS/ASP.NET abgeblendet (nicht verfügbar).

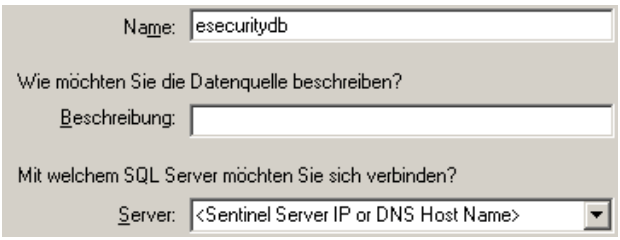


Konfiguration von Open Database Connectivity (ODBC) für SQL-Authentifizierung

Hiermit wird ein Open Database Connectivity-(ODBC-)Datenquellenname eingerichtet, damit Crystal Reports Server über die SQL-Authentifizierung die Verbindung mit der Sentinel-Datenbank herstellen kann (unter Windows und SQL Server). Diese Schritte müssen auf dem Computer durchgeführt werden, auf dem Crystal Reports Server installiert ist.

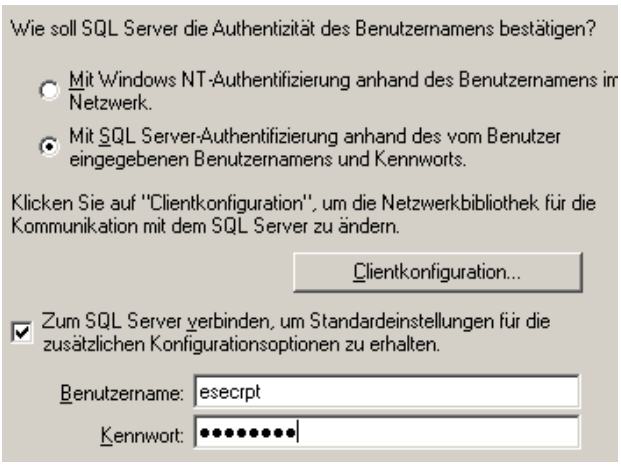
So richten Sie eine ODBC-Datenquelle für Windows ein:

1. Wechseln Sie zu Windows-Systemsteuerung > Verwaltung > Datenquellen (ODBC).
2. Klicken Sie auf die Registerkarte „System-DSN“ und dann auf „Hinzufügen“.
3. Wählen Sie SQL Server. Klicken Sie auf Fertig stellen.
4. Daraufhin wird ein Fenster angezeigt, in dem Sie zur Eingabe von Informationen zur Treiberkonfiguration aufgefordert werden.
   - Name der Datenquelle, geben Sie „esecuritydb“ ein
   - Feld „Description“ (Beschreibung) (optional); geben Sie eine Beschreibung ein
   - Feld „Server“ (Server); geben Sie Ihren Hostnamen bzw. die IP-Adresse Ihrer Instanz von Sentinel Server ein



Klicken Sie anschließend auf "Weiter".

5 Wählen Sie im nächsten Febster die Option für die SQL-Authentifizierung. Geben Sie „esecrpt“ und das zugehörige Passwort als Anmelde-ID ein. Klicken Sie anschließend auf "Weiter".


Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.
Klicken Sie auf "Clientkonfiguration", um die Netzwerkbibliothek für die Kommunikation mit dem SQL Server zu ändern.
Clientkonfiguration...
Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten.
Benutzername: esecrpt
Kennwort: ••••••••

6 Gehen Sie im nächsten Fenster wie folgt vor:

- Ändern Sie die Sentinel-Datenbank (Standardname: „ESEC“)
- Behalten Sie alle Standardeinstellungen bei.

Klicken Sie auf „Next“ (Weiter) und dann auf „Finish“ (Fertig stellen).

7 Klicken Sie auf „Test Data Source“ (Datenquelle testen). Nach dem Testen klicken Sie auf „OK“. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

8.7.3 Installation von Crystal Reports Server für Oracle

So installieren Sie Crystal Reports Server XI R2 für Oracle:

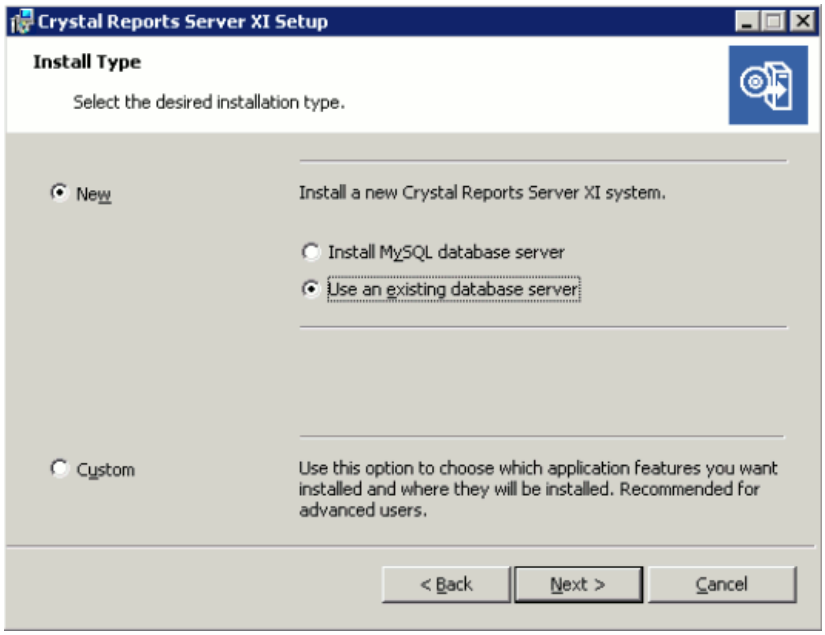
1 Legen Sie die Crystal Reports Server XI R2-CD in das CD-ROM-Laufwerk ein.

2 Wählen Sie die Sprache für das Crystal Reports-Setup aus.

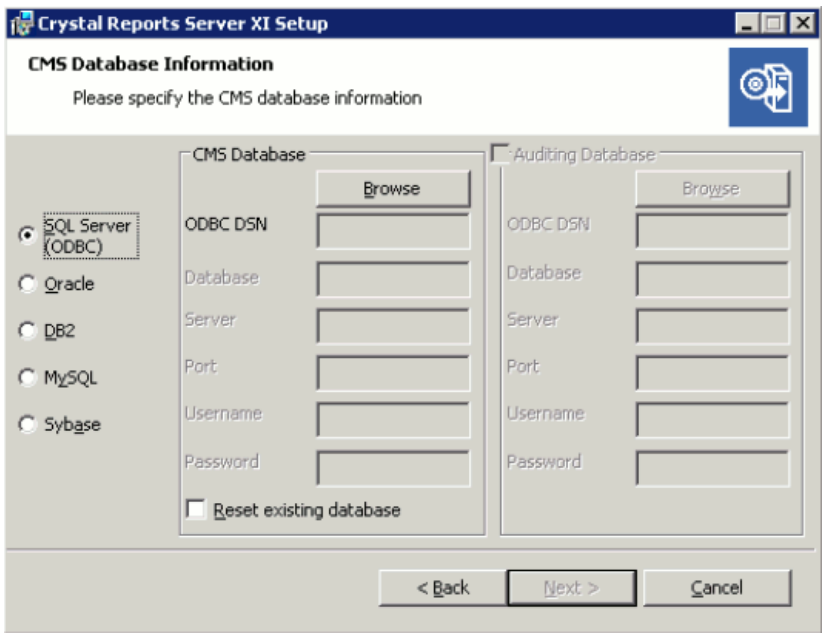
3 Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option „Perform Server Installation“ (Serverinstallation durchführen) aus.

Clientinstallation
Publishing-Assistent, Business Views Manager, Import-Assistent und SDKs
Serverinstallation
Installiert alle Komponenten einschließlich des Client SDKs.

4 Wählen Sie „Use an existing database server“ (Bestehenden Datenbankserver verwenden) aus.


Crystal Reports Server XI Setup
Install Type
Select the desired installation type.
New
Install a new Crystal Reports Server XI system.
Install MySQL database server
Use an existing database server
Custom
Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.
< Back
Next >
Cancel

Daraufhin wird das Fenster mit den Informationen zur CMS-Datenbank angezeigt:



Wählen Sie als Typ „SQL Server (ODBC)“ aus und klicken Sie auf „Browse“ (Durchsuchen), um einen DSN auszuwählen. Nach Auswahl des DSN werden Sie zur Eingabe von Benutzername und Passwort aufgefordert. Machen Sie die erforderlichen Angaben und klicken Sie dann auf „Next“ (Weiter).

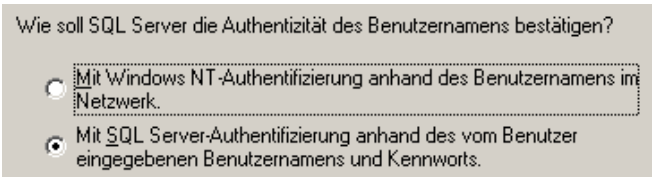
Hinweis: Crystal Reports Server und Microsoft SQL Server 2005 müssen sich auf demselben Computer befinden.

5 Wählen Sie IIS/ASP.NET aus.

Hinweis: Wenn Sie IIS und ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert haben, ist IIS/ASP.NET abgeblendet (nicht verfügbar). Die Installation von IIS und ASP.NET ist für diese Installation Voraussetzung.

Would you like to use:
Java application server
Use preinstalled Java application server (BEA WebLogic, IBM WebSphere, Oracle, SunOne, Tomcat, etc.)
*manual configuration required
Install Tomcat application server
IIS ASP.NET

6 Sie werden zur Eingabe des Authentifizierungsmodus aufgefordert. Wählen Sie die SQL Server-Authentifizierung aus.


Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.

Crystal Reports Server unterstütz den direkten Zugriff auf eine Sentinel-Datenbank unter Oracle. Diese Zugriffsfähigkeit wird durch die crdb_oracle.dll-Übersetzungsdatei gewährleistet. Diese Datei kommuniziert mit dem Oracle-Datenbanktreiber, der direkt mit Oracle-Datenbanken und -Clients zusammenarbeitet und die für Ihren Bericht erforderlichen Daten abruft.

Hinweis: Damit Crystal Reports Server Oracle-Datenbanken verwenden kann, muss die Oracle-Client-Software auf Ihrem System installiert sein und der Standort des Oracle-Client muss in der Umgebungsvariablen PATH angegeben sein.

Installation und Konfiguration der Oracle-Client-Software

Bei der Installation von Oracle Client:

- Übernehmen Sie das Standardinstallationsverzeichnis
- Wählen Sie „No“ (Nein) bei „Perform Typical Configuration“ (Typische Konfiguration durchführen)
- Wählen Sie „No“ (Nein) bei „Directory Service“ (Verzeichnisdienst)

- Wählen Sie Local (Lokal)
- TNS-Servicename: ESEC
- Benutzer (optional): esecrpt

Erstellen Sie nach der Installation eine lokale Net Service Name-Konfiguration.

Die nachfolgenden Anweisungen beziehen sich auf den systemeigenen Oracle 9-Treiber, sollten jedoch für Oracle 10 ähnlich sein.

So erstellen Sie eine Net Service Name-Konfiguration (Konfiguration des systemeigenen Oracle 9-Treibers:

1. Wählen Sie Oracle-OraHome92 > Configuration and Migration Tools (Konfigurations- und Migrationswerkzeuge) > Net Manager.
2. Erweitern Sie im Navigationsfenster „Local“ (Lokal) und markieren Sie „Service Naming“ (Service-Benennung).
3. Klicken Sie auf das Pluszeichen auf der linken Seite, um einen Service-Namen hinzuzufügen.
4. Geben Sie im Fenster „Service Name“ (Service-Name) einen Net Service-Namen ein.
   - Geben Sie „ESECURITYDB“ ein.

   Klicken Sie anschließend auf "Weiter".
5. Wählen Sie im Fenster „Select Protocols“ (Protokolle auswählen) den Standardwert aus:
   - TCP/IP (Internet Protocol)

   Klicken Sie anschließend auf "Weiter".
6. Hostname und Portnummer:
   - Geben Sie den Hostnamen bzw. die IP-Adresse des Computers ein, auf dem sich die Sentinel-Datenbank befindet.
   - Wählen Sie „Oracle Port“ (Oracle-Port) aus (standardmäßig 1521 bei der Installation)

   Klicken Sie anschließend auf "Weiter".
7. So identifizieren Sie die Sentinel-Datenbank bzw. den Sentinel-Service:
   - Wählen Sie „Oracle8i or later“ (Oracle8i oder höher) aus; geben Sie Ihren Service-Namen ein (dies ist der Name Ihrer Oracle-Instanz).
   - Wählen Sie als Verbindungstyp Database Default (Datenbankstandard) aus.

   Klicken Sie anschließend auf "Weiter".
8. Klicken Sie im Fenster „Test“ auf „Test“. Klicken Sie anschließend auf "Weiter". Möglicherweise ist der Test nicht erfolgreich, da dafür eine Datenbank-ID und ein Datenbankpasswort verwendet werden.
9. Wenn der Test nicht erfolgreich ist, gehen Sie wie folgt vor:
   - Klicken Sie im Fenster „Connection Test“ (Verbindungstest) auf „Change Login“ (Anmeldung ändern).
   - Geben Sie die Sentinel-Oracle-ID (verwenden Sie „esecrpt“) und das entsprechende Passwort ein. Klicken Sie auf "Testen".

Wenn der Test nicht erfolgreich ist:

- Senden Sie ein Ping-Signal an den Sentinel Server
- Vergewissern Sie sich, dass der Hostname des Sentinel Servers in der Hosts-Datei auf dem Crystal Reports Server vorliegt. Die Hosts-Datei finden Sie unter %SystemRoot%\system32\drivers\etc\.

10 Klicken Sie zunächst auf „Close“ (Schließen) und dann auf „Finish“ (Fertig stellen).

8.8 Konfiguration für alle Authentifizierungen und Konfigurationen

Folgende Schritte müssen durchgeführt werden, um die Zusammenarbeit von Crystal Reports Server und Sentinel Control Center zu ermöglichen.

8.8.1 Konfiguration von inetmgr

So konfigurieren Sie „inetmgr“:

1 Kopieren Sie die Datei `web.config` von:

`C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content`

nach c:\Inetpub\wwwroot.

2 Starten Sie Internet Service Manager durch Klicken auf Start > Ausführen. Geben Sie „inetmgr“ ein und klicken Sie auf „OK“.

3 Erweitern Sie (lokaler Computer) > Websites > Standardwebsite > businessobjects.

4 Klicken Sie bei businessobjects mit der rechten Maustaste > Eigenschaften.

5 Klicken Sie auf der Registerkarte „Virtual Directory“ (Virtuelles Verzeichnis) auf „Configuration“ (Konfiguration).

6 Folgende Zuordnungen sollten vorliegen. Wenn dies nicht der Fall ist, fügen Sie sie hinzu. Wenn Sie vorhaben, eine Zuordnung hinzuzufügen, klicken Sie nicht auf die Knoten businessobjects bzw. crystalreportsviewer11.

Erweiterung	Ausführbare Datei
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	...\BusinessObjects Enterprise 11.5

Klicken Sie auf OK, um das Fenster zu schließen.

7 Starten Sie IIS erneut. Gehen Sie dazu wie folgt vor: Erweitern Sie (lokaler Computer) > „Websites“ > „Standardwebsite“, markieren Sie „Standardwebsite“ und klicken Sie mit der rechten Maustaste > „Stop“.

8 Erweitern Sie (lokaler Computer) > „Websites“ > „Standardwebsite“, markieren Sie „Standardwebsite“ und klicken Sie mit der rechten Maustaste > „Start“.

8.9 Veröffentlichen Sie Crystal Reports-Schablonen

Viele Berichtsschablonen wurden von Novell für die Verwendung auf den Registerkarten „Analyse“ und „Advisor“ im Sentinel Control Center erstellt. Die neuesten Berichte können Sie von den Webseiten mit Sentinel 6-Inhalten unter folgender URL herunterladen:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

Die wichtigsten Sentinel-Berichte sind im Sentinel Core-Lösungspaket enthalten.

Sie haben vier Möglichkeiten, dem System Berichte hinzuzufügen:

- Laden Sie aus der Registerkarte „Lösungspakete“ ein Lösungspaket herunter und installieren Sie mithilfe des Lösungsmanagers mindestens ein Steuerelement, das Berichte enthält.
- Laden Sie aus der Registerkarte „Collectors“ ein Collector-Paket herunter und installieren Sie mithilfe des Lösungsmanagers mindestens ein Steuerelement, das Berichte enthält.
- Fügen Sie mithilfe des Crystal Publishing-Assistenten mindestens eine Berichtsschablone (.rpt-Dateien) hinzu.
- Fügen Sie mithilfe der Crystal Reports Central-Verwaltungskonsole mindestens eine Berichtsschablone (.rpt-Dateien) hinzu.

Wichtig: Zur Ausführung der Top 10-Berichte muss die Aggregation aktiviert und EventFileRedirectService in `DAS_Binary.xml` eingeschaltet sein. Diese Konfiguration ist bei der standardmäßigen Sentinel-Installation bereits gegeben. Informationen zur Aktivierung der Aggregierung erhalten Sie im Abschnitt “Konfiguration der Berichtsdaten” unter “Admin” im *Sentinel-Benutzerhandbuch*.

8.9.1 Veröffentlichen von Berichtsschablonen mit dem Lösungsmanager

Wurden Webserver und Crystal Reports-Server anhand der Installationsanweisungen in diesem Kapitel ordnungsgemäß konfiguriert, können in einem Lösungs- oder Collector-Paket enthaltene Berichte über den Lösungsmanager direkt in Crystal Reports Server veröffentlicht werden. Weitere Informationen finden Sie im Abschnitt zu “Solution Packs” im *Sentinel-Benutzerhandbuch*.

8.9.2 Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard

Sentinel-Berichte werden jetzt mithilfe von Lösungspaketen ausgeliefert. Sie können diese Methode aber auch zum Veröffentlichen von Berichtsschablonen verwenden, die nicht aus einem Lösungspaket stammen.

So veröffentlichen Sie die Crystal Report-Schablonen:

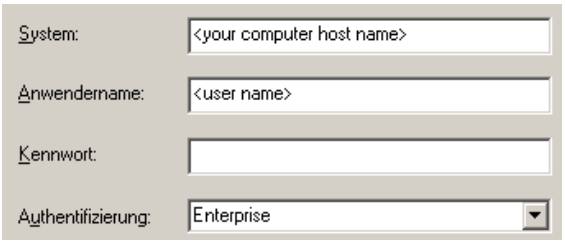
Hinweis: Wenn Sie Ihre Reports-Schablonen erneut veröffentlichen möchten, müssen Sie die zuvor importierten Reports-Vorlagen löschen.

1. Wählen Sie die Optionsfolge „Start“ > „Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „Publishing Wizard“.

   Klicken Sie anschließend auf "Weiter".

2. Anmelden. Bei „System“ (System) sollte der Hostname des Computers angegeben werden, auf dem Crystal installiert ist, und bei „Authentication“ (Authentifizierung) sollte „Enterprise“ angegeben werden. Der Benutzername kann „Administrator“ lauten. Aus Sicherheitsgründen sollten Sie unbedingt einen neuen Benutzer mit einem anderen Namen als „Administrator“ erstellen. Geben Sie Ihr Passwort ein und klicken Sie auf „Next“ (Weiter).

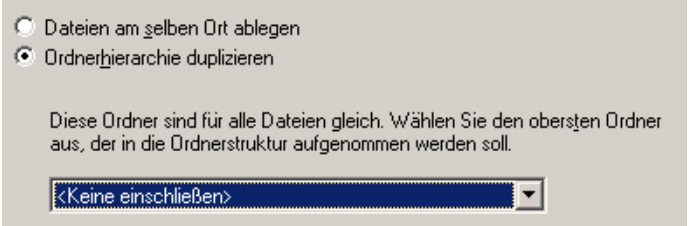
   Hinweis: Auf Berichte, die als Benutzer „Verwalter“ veröffentlicht wurden, haben alle Benutzer Zugriff.



3. Klicken Sie auf Ordner hinzufügen. [Optional] Wählen Sie „Unterordner einbeziehen“.
4. Navigieren Sie zum Verzeichnis der Berichtsschablone(n). Klicken Sie auf OK. Klicken Sie anschließend auf "Weiter".
5. Klicken Sie im Fenster „Standort angeben“ auf „Neuer Ordner“ in der oberen rechten Ecke und erstellen Sie einen Ordner „SentinelReports“, wenn dieser Ordner noch nicht vorhanden ist. Klicken Sie anschließend auf "Weiter".

6. Auswählen:
   - Duplicate the folder hierarchy (Ordnerhierachie duplizieren).

     Klicken Sie auf den nach unten weisenden Pfeild und wählen Sie „<include none>“ (<ohne Einfügung>) aus.



Klicken Sie anschließend auf "Weiter".

7 Klicken Sie im Fenster „Confirm Location“ (Speicherort bestätigen) auf Next (Weiter).

8 Geben Sie im Fenster „Kategorien angeben“ einen Kategorienamen an (z. B. Sentinel), markieren Sie den Namen und klicken Sie auf das Plussymbol.

Hinweis: Nur der erste Bericht wird nach dem Klicken auf „Next“ (Weiter) unter der Kategorie angezeigt.

Klicken Sie anschließend auf "Weiter".

9 Klicken Sie im Fenster „Specify Schedule“ (Zeitplan angeben) auf Let users update the object (Zulassen, dass Benutzer das Objekt aktualisieren) (sollte Standard sein). Klicken Sie anschließend auf "Weiter".

10 Klicken Sie im Fenster „Specify Repository Refresh“ (Repository-Aktualisierung angeben) auf Enable all (Alle aktivieren), um die Repository-Aktualisierung zu aktivieren. Klicken Sie anschließend auf "Weiter".

11 Klicken Sie im Fenster „Specify Keep Saved Data“ (Angabe für das Beibehalten gespeicherter Daten) auf Enable all (Alle aktivieren), um beim Veröffentlichen von Berichten die gespeicherten Daten beizubehalten. Klicken Sie anschließend auf "Weiter".

12 Klicken Sie im Fenster „Change Defaults Values“ (Standardwerte ändern) auf das Optionsfeld Publish reports without modifying properties (Berichte veröffentlichen, ohne Eigenschaften zu ändern) (sollte Standard sein). Klicken Sie anschließend auf "Weiter".

13 Klicken Sie auf Next (Weiter), um Ihre Objekte hinzuzufügen.

14 Es wird eine veröffentlichte Liste angezeigt; klicken Sie auf „Finish“ (Fertig stellen).

Wenn Sie die Sentinel-Schablonen für Crystal Reports im Crystal Reports Server veröffentlichen, müssen sich die Schablonen im Verzeichnis „SentinelReports“ befinden. Anderenfalls werden sie nicht im Sentinel Control Center angezeigt.

8.9.3 Veröffentlichen von Reports-Schablonen – Central Management Console

Sentinel-Berichte werden jetzt mithilfe von Lösungspaketen ausgeliefert. Sie können diese Methode aber auch zum Veröffentlichen von Berichtsschablonen verwenden, die nicht aus einem Lösungspaket stammen.

So importieren Sie Crystal Reports-Schablonen:

1 Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

```
http://<hostname_or_IP_of_web_server>/businessobjects/
enterprise115/WebTools/adminlaunch
```

2 Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).

3 Melden Sie sich bei Crystal Reports Server an.

4 Klicken Sie im Fenster „Organize“ (Organisieren) auf Folders (Ordner).

5 Klicken Sie in der rechten oberen Ecke auf „New Folder“ (Neuer Ordner).

6 Erstellen Sie einen Ordner „SentinelReports“, falls er nicht bereits vorhanden ist. Klicken Sie auf "OK".

Hinweis: Beim Namen des Ordners gab es keinerlei Abweichung von „SentinelReports“ geben.

---

7 Klicken Sie auf „SentinelReports“ (SentinelReports).

8 Klicken Sie auf die Registerkarte „Unterordner“ und erstellen Sie entsprechend Ihren Anforderungen Unterordner. Wenn Sie die Sentinel Core-Berichte manuell hinzufügen, erstellen Sie die folgenden Unterordner:

- Advisor_Vulnerability
- Dashboards
- Incident Management
- Internal Events
- Security Events
- Top 10

9 Wählen Sie die Optionsfolge „Home“ > „Objects“ > „New Object“ (Anfang > Objekte > Neues Objekt).

10 Markieren Sie auf der linken Seite den Eintrag „Report“ (Bericht).

11 Klicken Sie auf „Durchsuchen“ und navigieren Sie zum Verzeichnis der hinzuzufügenden Berichtsschablonen. Wählen Sie einen Ordner und darin einen Bericht aus.

12 Markieren Sie „SentinelReports“ und klicken Sie auf „Unterordner anzeigen“.

13 Wählen Sie den entsprechenden Ordner für den Bericht aus und klicken Sie auf Show Subfolders (Unterordner anzeigen).

14 Klicken Sie auf „Senden“.

15 Wenn Sie die restlichen Berichte hinzufügen möchten, wiederholen Sie Schritt 9 bis 17 so lange, bis alle Berichte hinzugefügt wurden.

8.9.4 Definieren eines benannten Benutzerkontos

Der im Lieferumfang von Crystal Reports Server enthaltene Schlüssel ist ein Kontoschlüssel für „Named User“ (Benannter Benutzer). Das Gastkonto muss von „Concurrent User“ (Gleichzeitiger Benutzer) in „Named User“ (Benannter Benutzer) geändert werden.

So definieren Sie das Gastkonto als „Named User“ (Benannter Benutzer):

1 Wählen Sie die Optionsfolge „Start“ > „Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „.NET Administration Launchpad“.

2 Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).

3 Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.

4. Geben Sie als Benutzernamen „Administrator“ ein. Geben Sie Ihr Passwort ein (standardmäßig leer). Klicken Sie auf Log On (Anmelden). Klicken Sie im Fenster „Organize“ (Organisieren) auf Users (Benutzer).
5. Klicken Sie auf Guest (Gast).
6. Ändern Sie den Verbindungstyp von Concurrent User (Gleichzeitiger Benutzer) in Named User (Benannter Benutzer).

   Wichtig: Um die Erstellung einer unbegrenzten Anzahl an Berichten zu ermöglichen, sollten Sie das Konto „Named User License“ (Benannte Benutzerlizenz) verwenden.
7. Klicken Sie auf "Aktualisieren".
8. Melden Sie sich ab und schließen Sie das Fenster oder gehen Sie weiter zum Abschnitt Konfigurieren von .NET Administration Launchpad.

8.9.5 Konfigurieren von Berichtsberechtigungen

Hier wird erläutert, wie Sie mit .NET Administration Launchpad die Berechtigungen für Berichte so konfigurieren können, dass Sie in der Lage sind, Berichte nach Bedarf anzuzeigen und zu bearbeiten.

So konfigurieren Sie Berichtsberechtigungen:

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad (Klicken Sie auf „Start“ > „Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „.NET Administration Launchpad“).

   Hinweis: Wenn beim Aufruf von .NET Administration Launchpad der „HTTP 404“-Fehler (Datei oder Verzeichnis nicht gefunden) ausgegeben wird, ziehen Sie hinsichtlich der Beseitigung http://support.microsoft.com/kb/315122 (http://support.microsoft.com/kb/315122) zurate.
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).

   Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
3. Geben Sie als Benutzernamen „Administrator“ ein. Geben Sie Ihr Passwort ein (standardmäßig leer). Klicken Sie auf Log On (Anmelden). Klicken Sie im Bereich „Organize“ (Organisieren) auf „Folders“ (Ordner).
4. Klicken Sie einmal auf „SentinelReports“.
5. Alles auswählen.
6. Klicken Sie auf den Karteireiter Rights (Rechte).
7. Wählen Sie im Dropdown-Menü direkt unterhalb von „Access Level“ (Zugriffsebene) für „Everyone“ (Alle) die Option View on Demand (Auf Verlangen anzeigen) aus.
8. Klicken Sie auf "Aktualisieren".
9. Melden Sie sich ab und schließen Sie das Fenster.

Testen auf Webserver-Verbindung mit der Sentinel-Datenbank

So testen Sie auf Webserver-Verbindung mit der Datenbank:

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad („Start“ > „Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „.NET Administration Launchpad“).
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Geben Sie als Benutzernamen „Administrator“ ein. Geben Sie Ihr Passwort ein (standardmäßig leer). Klicken Sie auf Log On (Anmelden).
4. Begeben Sie sich zu „Folders“ > „SentinelReports“ > „Internal Events“ (Ordner > SentinelReports > Interne Ereignisse).
5. Wählen Sie Column Display Details (Spaltenanzeigedetails) aus.
6. Klicken Sie auf Preview (Vorschau).
7. Melden Sie sich – je nach System – als „esecrpt“ oder als Sentinel Report-Benutzer an.
8. Wählen Sie im Dropdown-Menü für das Sortierfeld „Tag“ (Tag) aus.
9. Klicken Sie auf OK. Daraufhin wird ein Bericht angezeigt.

Testen der Konnektivität zum Webserver

So testen Sie die Konnektivität zum Webserver:

1. Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.
2. Geben Sie

   ```
   http://<DNS name or IP address of your web server>/businessobjects/
   enterprise115/WebTools/adminlaunch/default.aspx
   ```

Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

8.9.6 Deaktivieren von Sentinel Top 10-Berichten

Standardmäßig sind Sentinel Top 10-Berichte aktiviert. Wenn Sie diese Berichte aller Voraussicht nach nicht benötigen, können Sie den Datenbankspeicher und die CPU-Verwendung verringern, indem Sie die Sentinel Top 10-Berichte deaktivieren:

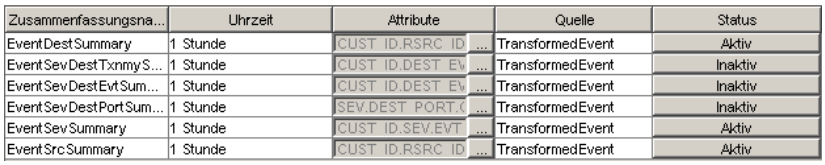
- Aggregation deaktivieren
- EventFileRedirectService deaktivieren

So deaktivieren Sie die Aggregation:

1. Rufen Sie das Sentinel Control Center auf.
2. Anmelden.
3. Klicken Sie auf die Admin-Registerkarte und wählen Sie die Option „Reporting Data“ (Berichtdaten).
4. Deaktivieren Sie folgende Zusammenfassungen:
   - EventDestSummary

- EventSevSummary
- EventSrcSummary

Klicken Sie in der Spalte „Status“ (Status) auf „Active“ (Aktiv), bis sich der Wert in „InActive“ (Inaktiv) ändert.



Zusammenfassungsna...	Uhrzeit	Attribute	Quelle	Status
EventDestSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv
EventSevDestTxnmyS...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestEvtSum...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestPortSum...	1 Stunde	SEV.DEST_PORT.(...	TransformedEvent	Inaktiv
EventSevSummary	1 Stunde	CUST_ID.SEV.EVT ...	TransformedEvent	Aktiv
EventSrcSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv

So deaktivieren Sie EventFileRedirectService:

1 Öffnen Sia auf Ihrem DAS-Computer mithilfe des Texteditors folgende Datei:

Bei UNIX:

```
$ESEC_HOME/config/das_binary.xml
```

Für Windows:

```
%ESEC_HOME%\config\das_binary.xml
```

2 Ändern Sie den Status von EventFileRedirectService in „Off“ (Aus).

```
<property name="status">off</property>
```

3 Starten Sie die DAS-Komponente folgendermaßen erneut:

Unter Windows:

```
Use Service Manager to stop and then start the "sentinel" service
```

8.9.7 Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server

Sentinel Control Center kann zur Integration in Crystal Reports Server konfiguriert werden, Sie können dann also Crystal Reports in Sentinel Control Center anzeigen.

Gehen Sie zur Integration des Sentinel Control Centers in Crystal Reports Server wie nachfolgend beschrieben vor.

Hinweis: Diese Konfiguration darf erst durchgeführt werden, nachdem Crystal Reports Server installiert und Crystal Reports in dieser Anwendung veröffentlicht wurden.

So konfigurieren Sie Sentinel zur Integration in Crystal Reports Server:

1 Melden Sie sich bei Sentinel Control Center als Benutzer mit Rechten für die Registerkarte „Admin“ an.

2 Wählen Sie auf der Registerkarte „Admin“ die Option „Konfiguration für Crystal-Bericht“.

3 Geben Sie in das Feld „Analyse-URL“ Folgendes ein:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Hinweis: <hostname_oder_IP_von_webserver> muss durch die IP-Adresse bzw. den Hostnamen von Crystal Reports Server ersetzt werden.

Hinweis: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn der APS auf die IP-Adresse gesetzt ist. Es muss sich um den Crystal Reports Server-Hostnamen handeln.

4 Klicken Sie neben dem Feld „Analyse-URL“ auf Aktualisieren.

5 Wenn Advisor auf Ihrem Computer installiert ist, geben Sie Folgendes in das Feld „Advisor-URL“ ein:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Hinweis: „<hostname_oder_IP_von_webserver>“ muss durch die IP-Adresse bzw. den Hostnamen von Crystal Reports Server ersetzt werden.

Hinweis: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS die IP-Adresse angegeben ist. Es muss sich um den Crystal Reports Server-Hostnamen handeln.

6 Klicken Sie neben dem Feld „Advisor URL“ auf Aktualisieren.

7 Klicken Sie auf "Speichern".

8 Melden Sie sich beim Sentinel Control Center ab und erneut wieder an. Die Crystal Reports-Bäume auf den Registerkarten „Analyse“ und „Advisor“ (wenn Advisor installiert ist) sollten nun im Navigatorfenster angezeigt werden.

8.10 Auf Hochleistung ausgerichtete Konfigurationen für Crystal

8.10.1 Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung

Je nachdem, wie viele Ereignisse Crystal abfragt, erhalten Sie möglicherweise eine Fehlermeldung bezüglich der maximalen Verarbeitungszeit oder der maximalen Datensatzgrenze. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren. Dieser Vorgang kann entweder über Central Configuration Manager oder über die Crystal-Webseite durchgeführt werden.

So konfigurieren Sie Crystal Page Server über Central Configuration Manager neu:

1 Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.

2 Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und wählen Sie „Stopp“.

3 Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und wählen Sie „Properties“ (Eigenschaften).

4 Fügen Sie auf dem Karteireiter „Properties“ (Eigenschaften) im Feld „Command“ (Befehl) am Ende der Befehlszeile Folgendes hinzu:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the
default limit>
```

5 Starten Sie Crystal Page Server neu.

So konfigurieren Sie Crystal Page Server über die Central-Verwaltungskonsole neu:

1. Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects 11“ > „Crystal Reports Server“ > „.NET Administration Launchpad“. Sie können auch einen Webbrowser öffnen und die folgende URL eingeben:

   http://<DNS-Name oder IP-Adresse Ihres Webservers>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort an und klicken Sie auf „Log On“ (Anmelden). Klicken Sie auf Servers (Server).
5. Klicken Sie auf „<server name>.pageserver“.
6. Klicken Sie unter „Database Records to Read When Previewing Or Refreshing a report“ (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf „Unlimited records“ (Unbegrenzt viele Datensätze). Klicken Sie auf "Anwenden".
7. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf „OK“.

Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager des Betriebssystems aufgefordert.

8.10.2 Berichte, die den Aggregationsdienst verwenden.

Zur Verbesserung der Leistung fragen die 10 wichtigsten im Sentinel Core Solution Pack enthaltenen Berichte Zusammenfassungstabellen anstatt der Ereignistabelle ab. Die Zusammenfassungstabellen enthalten mit der Zeit Zahlen für Kombinationen von Feldern in den Ereignisdaten. Dies bietet einen wesentlich geringeren Datensatz für bestimmte Abfragetypen und führt zu viel schnelleren Abfragen und Berichtslaufzeiten.

Der Aggregationsdienst ist für das Auffüllen der Zusammenfassungstabellen mit Zusammenfassungen der Ereignisse in der Ereignistabelle verantwortlich. Der Aggregationsdienst generiert nur zusammengefasste Daten für Zusammenfassungen, die aktiv sind. Die folgenden Zusammenfassungen werden von den Top 10-Berichten benötigt und sind standardmäßig aktiviert:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Zusammenfassungen können mithilfe des Fensters zur Konfiguration von Berichtsdaten unter der Registerkarte „Admin“ vom Sentinel Control Center aktiviert bzw. deaktiviert werden.

Der Aggregationsdienst ist außerdem von der Komponente `EventFileRedirectService` in DAS Binary abhängig, um ihm die Ereignisdaten bereitzustellen, die es zusammenfasst. Deshalb muss diese Komponente aktiviert werden, damit der Aggregationsdienst ordnungsgemäß ausgeführt wird. Diese Komponente wird durch Ändern des Attributs „status“ der Komponente `EventFileRedirectService` in der Datei `das_binary.xml` aktiviert bzw. deaktiviert. Standardmäßig ist diese Komponente aktiviert.

Hinweis: Informationen zu EventFileRedirectService und den drei Aggregierungszusammenfassungen erhalten Sie in “Konfiguration der Berichtsdaten” in „Admin“ im *Sentinel-Benutzerhandbuch*.

Hinweis: Berichte, die einen großen Datenbereich abfragen, nehmen eventuell einige Zeit in Anspruch. Sie können geplant und nicht interaktiv ausgeführt werden. Informationen zur Planung von Crystal Reports finden Sie in der Dokumentation zu Crystal BusinessObjects Enterprise™ 11 (http://support.businessobjects.com/documentation/product_guides/default.asp).

8.10.3 Report Development

Der Crystal Reports Developer kann zum Erstellen oder Ändern von Crystal-Berichten verwendet werden. Für benutzerdefinierte entwickelte Berichte wird Folgendes empfohlen:

- Wenn die Berichte vordefinierte aggregierte Tabellen verwenden können, wählen Sie diejenige aggregierte Tabelle aus, bei der die wenigsten Daten verarbeitet werden.
- Versuchen Sie, einen möglichst großen Teil der Verarbeitung auf die Datenbank-Engine zu verlagern.
- Um den Verarbeitungs-Overhead in Crystal Server zu verringern, sollten Sie die in Crystal Server zu ladende Datenmenge so gering wie möglich halten.
- Schreiben Sie Berichte immer anhand der von Novell bereitgestellten Datenbankansichten und nicht anhand der Basistabellen.

Crystal Reports für Linux

9

- Abschnitt 9.1, „Überblick“, auf Seite 132
- Abschnitt 9.2, „Installation“, auf Seite 132
- Abschnitt 9.3, „Veröffentlichen von Crystal Reports-Schablonen“, auf Seite 136
- Abschnitt 9.4, „Verwenden von Crystal XI R2 Web Server“, auf Seite 139
- Abschnitt 9.5, „Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung“, auf Seite 141
- Abschnitt 9.6, „Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server“, auf Seite 142
- Abschnitt 9.7, „Dienstprogramme und Fehlersuche“, auf Seite 143
- Abschnitt 9.8, „Auf Hochleistung ausgerichtete Konfigurationen für Crystal“, auf Seite 145

Crystal Reports Server™ (von Business Objects) ist das zusammen mit Sentinel verwendete Berichterstellungswerkzeug. In diesem Abschnitt wird die Installationskonfiguration von Crystal Reports Server für Sentinel erörtert. Weitere Informationen zu den unterstützten Plattformen für Crystal Reports Server in einer Sentinel-Umgebung finden Sie in Kapitel 2, „Systemanforderungen“, auf Seite 21.

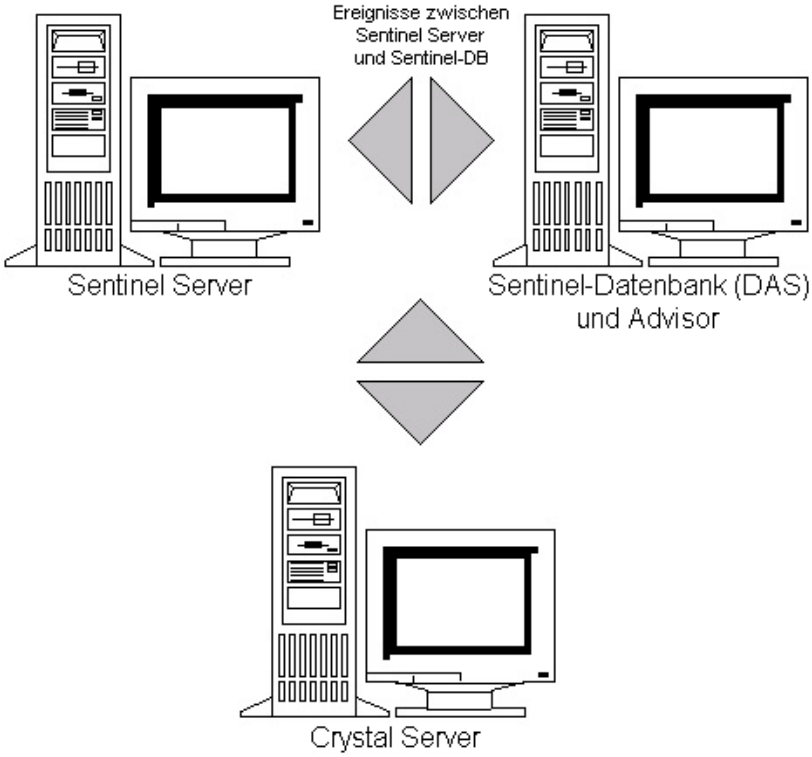
Unter Linux wurde Sentinel zusammen mit Crystal Reports Server XI R2 SP2 getestet. Weitere Informationen zu Crystal Reports Server XI Release 2 Service Packs bzw. die Packs zum Download erhalten Sie unter https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads). Suchen Sie dort nach der gewünschten Version und Plattform.

In diesem Abschnitt wird die Ausführung von Crystal Reports Server unter Linux behandelt. Weitere Informationen zur Ausführung von Crystal Reports Server unter Windows finden Sie in Kapitel 8, „Crystal Reports für Windows“, auf Seite 101.

Wichtig: Die Installation sollte in der unten angegebenen Reihenfolge vorgenommen werden.

So installieren Sie Crystal Reports Server:

1. Vorinstallation und Installation von Crystal Reports Server™ XI R2
2. Anwenden von Patches für Crystal Reports Server
3. Veröffentlichen (Importieren) von Crystal Reports-Berichten
4. Festlegen eines Kontos für einen benannten Benutzer
5. Testen der Konnektivität zum Webserver
6. Aktivieren der Top 10-Berichte (optional)
7. Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung (empfohlen)
8. Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server



9.1 Überblick

Crystal Reports Server benötigt eine Datenbank zum Speichern von Informationen über das System und dessen Benutzer. Diese Datenbank ist als Central Management Server-(CMS-)Datenbank bekannt. Der CMS ist ein Server, der Informationen über das Crystal Reports Server-System speichert. Nach Bedarf können weitere Komponenten von Crystal Reports Server Zugriff auf diese Informationen erlangen.

9.2 Installation

9.2.1 Vorinstallation von Crystal Reports Server™ XI R2

So führen Sie die Vorinstallation von Crystal Reports Server durch:

1. Wenn sich die Sentinel-Datenbank nicht auf demselben Computer befindet wie Crystal Reports Server, müssen Sie die Oracle Client-Software auf dem Computer mit Crystal Reports Server installieren. Dieser zusätzliche Schritt ist nicht erforderlich, wenn sich die Sentinel-Datenbank auf demselben Computer befindet wie Crystal Reports Server, da die erforderliche Oracle-Software in diesem Fall bereits während der Oracle-Datenbank-Installation installiert wurde.
2. Melden Sie sich als Benutzer „root“ beim Crystal Reports Server-Computer an.
3. Erstellen Sie die Gruppe „bobje“.

   ```
   groupadd bobje
   ```

4. Erstellen Sie den Crystal-Benutzer (das Basisverzeichnis ist in diesem Fall „/export/home/crystal“, ändern Sie es, falls erforderlich; der Teil „/export/home“ des Pfads muss bereits vorhanden sein).

   ```
   useradd -g bobje -s /bin/bash -d /export/home/crystal -m crystal
   ```

5. Erstellen Sie ein Verzeichnis für die Crystal-Software:

   ```
   mkdir -p /opt/crystal_xir2
   ```

6. Ändern Sie den Eigentümer des Verzeichnisses für die Crystal-Software (rekursiv) in crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xir2
   ```

7. Sie müssen mithilfe einer Zugriffssteuerungsliste (Access Control List, ACL) dem Crystal-Benutzer im Verzeichnis „$ORACLE_HOME“ Berechtigungen erteilen. Angenommen der Benutzer ist „crystal“ und „$ORACLE_HOME“ ist `/opt/oracle/product/10.2/db_1`, dann lautet der zugehörige Befehl:

   ```
   setfacl -m u:crystal:rx -R  /opt/oracle/product/10.2/db_1
   ```

   Um zu überprüfen, ob die ACL ordnungsgemäß festgelegt wurde, führen Sie folgenden Befehl aus und suchen Sie in der Ausgabe nach „crystal“:

   ```
   getfacl  /opt/oracle/product/10.2/db_1
   ```

8. Wechseln Sie zum Crystal-Benutzer:

   ```
   su - crystal
   ```

9. Die Umgebungsvariable ORACLE_HOME muss in der Umgebung des Crystal-Benutzers festgelegt werden. Bearbeiten Sie dazu das Anmeldeskript des Crystal-Benutzers, um die Umgebungsvariable ORACLE_HOME auf die Basis der Oracle-Software zu setzen. Beispiel: Wenn es sich bei der Shell eines Crystal-Benutzers um eine Bash-Shell handelt und die Oracle-Software im Verzeichnis `/opt/oracle/product/10.2/db_1` installiert ist, müssen Sie die Datei `~crystal/.bash_profile` (`.profile` auf SLES) öffnen und folgende Zeile am Ende der Datei einfügen:

   ```
   export ORACLE_HOME=/opt/oracle/product/10.2/db_1
   ```

10. Die Umgebungsvariable LD_LIBRARY_PATH in der Umgebung des Crystal-Benutzers muss den Pfad zu den Oracle-Softwarebibliotheken enthalten. Bearbeiten Sie dazu das Anmeldeskript des Crystal-Benutzers, um die Umgebungsvariable LD_LIBRARY_PATH so festzulegen, dass sie die Oracle-Softwarebibliotheken enthält. Beispiel: Wenn es sich bei der Shell eines Crystal-Benutzers um eine Bash-Shell handelt, müssen Sie die Datei `~crystal/.bash_profile` öffnen und folgende Zeile am Ende der Datei (unterhalb der Stelle, an der die Umgebungsvariable „ORACLE_HOME“ festgelegt wurde) einfügen:

    ```
    export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
    ```

11. Die Umgebungsvariable „_PATH“ in der Umgebung des Crystal-Benutzers muss den Pfad zu den ausführbaren Oracle-Softwaredateien enthalten. Bearbeiten Sie dazu das Skript des Crystal-Benutzers, um die Umgebungsvariable „_PATH“ so festzulegen, dass sie die ausführbaren Oracle-Softwaredateien enthält. Beispiel: Wenn es sich bei der Shell eines Crystal-Benutzers um eine Bash-Shell handelt, müssen Sie die Datei `~crystal/.bash_profile` öffnen und folgende Zeile am Ende der Datei einfügen:

    ```
    export PATH=$PATH:$ORACLE_HOME/bin
    ```

12. Es muss ein Eintrag mit dem Servicenamen „esecuritydb“ zur Oracle-Datei `tnsnames.ora` hinzugefügt werden, der auf die Sentinel-Datenbank verweist. Gehen Sie dazu auf dem Crystal Reports Server-Computer wie folgt vor:

    12a Melden Sie sich als Oracle-Benutzer an.

12b Wechseln Sie in das Verzeichnis $ORACLE_HOME/network/admin

12c Erstellen Sie eine Sicherungskopie der Datei `tnsnames.ora`.

12d Öffnen Sie die Datei `tnsnames.ora` zur Bearbeitung.

12e Wenn sich die Sentinel-Datenbank auf dem Crystal Reports Server-Computer befindet, sollte bereits ein Eintrag in der Datei `tnsnames.ora` vorhanden sein, der auf die Sentinel-Datenbank verweist. Wenn die Sentinel-Datenbank beispielsweise den Namen ESEC trägt, ist ein Eintrag wie der folgende vorhanden:

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12f Wenn sich die Sentinel-Datenbank nicht auf dem Crystal Reports Server-Computer befindet, öffnen Sie die Datei `tnsnames.ora` auf dem Computer mit der Sentinel-Datenbank, um den oben beschriebenen Eintrag zu finden.

12g Erstellen Sie eine Kopie des gesamten Eintrags und fügen Sie ihn am Ende der Datei `tnsnames.ora` auf dem Crystal Reports Server-Computer ein. Der Teil des Eintrags für den Service-Namen muss in `esecuritydb` umbenannt werden. Wenn beispielsweise der obige Eintrag kopiert und ordnungsgemäß umbenannt wurde, sieht er folgendermaßen aus:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12h Achten Sie darauf, dass der HOST-Teil des Eintrags korrekt ist (stellen Sie beispielsweise sicher, dass er nicht auf „localhost“ gesetzt ist, wenn sich Crystal Reports Server und die Sentinel-Datenbank auf verschiedenen Computern befinden).

12i Speichern Sie die Änderungen an der Datei `tnsnames.ora`..

12j Führen Sie folgenden Befehl aus, um zu überprüfen, ob der Service-Name `esecuritydb` ordnungsgemäß konfiguriert wurde:

```
tnsping esecuritydb
```

12k Nach der Ausführung des Befehls erhalten Sie eine Meldung, die besagt, dass die Verbindung in Ordnung ist.

9.2.2 Installation von Crystal Reports Server XI R2

Das Installationsprogramm von Crystal Reports Server besteht aus zwei `.iso`-Dateien. Während der Installation werden Sie aufgefordert, den Standort des zweiten Datenträgers anzugeben.

So installieren Sie Crystal Reports Server:

1. Melden Sie sich als Crystal-Benutzer an.
2. Wechseln Sie in das Verzeichnis „disk1“ des Crystal-Installationsprogramms.
3. Ausführen:
   `./install.sh`
4. Wählen Sie als Sprache „English“ (Englisch) aus.
5. Wählen Sie „New Installation“ (Neue Installation).
6. Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.
7. Geben Sie den Schlüsselcode des Produkts ein.
8. Geben Sie das Installationsverzeichnis an:
   `/opt/crystal_xir2`
9. Wählen Sie die Option „User install“ (Benutzerinstallation).
10. Wählen Sie die Option „New install“ (Neuinstallation).
11. Wählen Sie die Option „Install MySQL“ (MySQL installieren), es sei denn, Sie haben vor, die Crystal CMS-Datenbank in einer bestehenden Datenbank zu installieren.
12. Geben Sie Konfigurationsinformationen für MySQL an:
    - **12a** „Use default port 3306“ (Standardport 3306 verwenden)
    - **12b** „Admin password“ (Administrator-Passwort)
13. Geben Sie weitere Konfigurationsinformationen für MySQL an:
    - **13a** „Default DB Name“ (Standarddatenbankname): „BOE115“
    - **13b** „User id“ (Benutzer-ID): „mysqladm“
    - **13c** Passwort
14. Geben Sie weitere Konfigurationsinformationen für MySQL an:
    - **14a** „Local Name Server“ (Lokaler Namensserver): <Hostname des lokalen Computers>
    - **14b** „Default CMS Port Number“ (CMS-Standard-Portnummer): „6400“
15. Wählen Sie die Option „Install Tomcat“ (Tomcat installieren).
16. Geben Sie Tomcat-Konfigurationsinformationen an:
    - **16a** „Default Receive HTTP requests port“ (Standardport zum Empfangen von HTTP-Anforderungen): „8080“
    - **16b** „Default Redirect jsp requests port“ (Standardport für die Umleitung von jsp-Anforderungen): „8443“
    - **16c** „Default Shutdown Hook port“ (Standardport für Herunterfahren des Hook): „8005“
17. Drücken Sie die Eingabetaste, um das Standardverzeichnis zu bestätigen.
18. Drücken Sie die Eingabetaste, um den Installationsvorgang zu starten.
19. Beachten Sie den Link zum CMS-Server, der ungefähr wie folgt lauten dürfte:
    http://<hostname>:8080/businessobjects/enterprise115/adminlaunch/launchpad.html

9.3 Veröffentlichen von Crystal Reports-Schablonen

Hinweis: Es wird dringend empfohlen, vor der Ausführung dieser Aufgabe die Versionshinweise zu Sentinel Reports zu lesen. Möglicherweise wurden Dateien oder Skripts aktualisiert oder Schritte hinzugefügt.

Viele Berichtsschablonen wurden von Novell für die Verwendung auf den Registerkarten „Analyse“ und „Advisor“ im Sentinel Control Center erstellt. Die neuesten Berichte können Sie von den Webseiten mit Sentinel 6-Inhalten unter folgender URL herunterladen:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

Die wichtigsten Sentinel-Berichte sind im Sentinel Core-Lösungspaket enthalten.

Sie haben vier Möglichkeiten, dem System Berichte hinzuzufügen:

- Laden Sie aus der Registerkarte „Lösungspakete“ ein Lösungspaket herunter und installieren Sie mithilfe des Lösungsmanagers mindestens ein Steuerelement, das Berichte enthält.
- Laden Sie aus der Registerkarte „Collectors“ ein Collector-Paket herunter und installieren Sie mithilfe des Lösungsmanagers mindestens ein Steuerelement, das Berichte enthält.
- Fügen Sie mithilfe des Crystal Publishing-Assistenten mindestens eine Berichtsschablone (.rpt-Dateien) hinzu.
- Fügen Sie mithilfe der Crystal Reports Central-Verwaltungskonsole mindestens eine Berichtsschablone (.rpt-Dateien) hinzu.

Wichtig: Zur Ausführung von Top 10-Berichten muss die Aggregation aktiviert und EventFileRedirectService in `DAS_Binary.xml` eingeschaltet sein. Informationen zur Aktivierung der Aggregierung erhalten Sie im Abschnitt “Konfiguration der Berichtsdaten” unter “Admin” im *Sentinel-Benutzerhandbuch*.

9.3.1 Veröffentlichen von Berichtsschablonen mit dem Lösungsmanager

Wurden Webserver und Crystal Reports-Server anhand der Installationsanweisungen in diesem Kapitel ordnungsgemäß konfiguriert, können in einem Lösungs- oder Collector-Paket enthaltene Berichte über den Lösungsmanager direkt in Crystal Reports Server veröffentlicht werden. Weitere Informationen finden Sie im Abschnitt zu “Solution Packs” im *Sentinel-Benutzerhandbuch*.

9.3.2 Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard

Sentinel-Berichte werden jetzt mithilfe von Lösungspaketen ausgeliefert. Sie können diese Methode aber auch zum Veröffentlichen von Berichtsschablonen verwenden, die nicht aus einem Lösungspaket stammen.

Hinweis: Zur Ausführung von Crystal Publishing Wizard ist eine Windows-Plattform erforderlich.

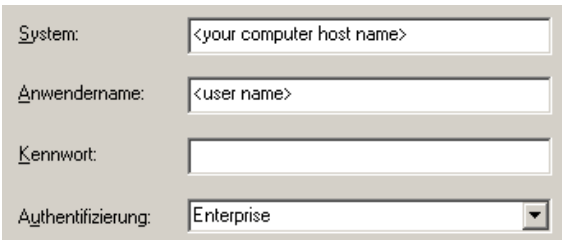
So importieren Sie Crystal Reports-Schablonen:

Hinweis: Wenn Sie Ihre Reports-Schablonen erneut importieren (veröffentlichen), müssen Sie den vorherigen Schablonen-Import löschen.

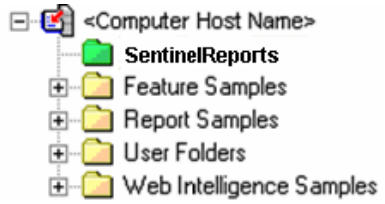
1. Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects 115“ > „Crystal Reports Server“ > „Publishing Wizard“.
2. Klicken Sie anschließend auf "Weiter".

   Anmelden. Als System sollte der Name des Host-Computers verwendet werden und als Authentifizierung „Enterprise“. Der Benutzername kann „Administrator“ lauten. Aus Sicherheitsgründen sollten Sie einen anderen Benutzer verwenden als den Administrator. Geben Sie Ihr Passwort ein und klicken Sie auf „Next“ (Weiter).

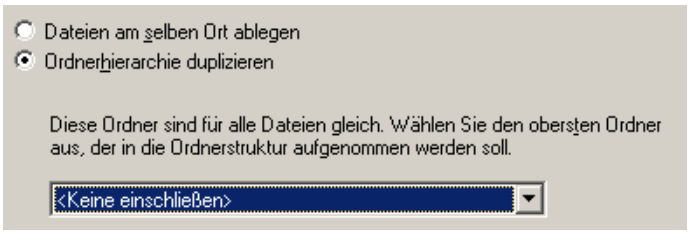
   Hinweis: Auf Berichte, die als Benutzer „Verwalter“ veröffentlicht wurden, haben alle Benutzer Zugriff.



3. Klicken Sie auf Ordner hinzufügen. [Optional] Wählen Sie „Unterordner einbeziehen“.
4. Navigieren Sie zum Verzeichnis der Berichtsschablone(n). Klicken Sie auf OK. Klicken Sie anschließend auf "Weiter".
5. Klicken Sie im Fenster „Standort angeben“ auf „Neuer Ordner“ in der oberen rechten Ecke und erstellen Sie einen Ordner „SentinelReports“, wenn dieser Ordner noch nicht vorhanden ist. Klicken Sie anschließend auf "Weiter".



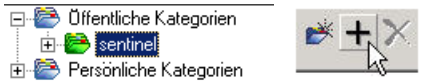
6. Auswählen:
   - Duplicate the folder hierarchy (Ordnerhierachie duplizieren).
   - Klicken Sie auf den nach unten weisenden Pfeild und wählen Sie „<include none>“ (<ohne Einfügung>) aus.



Klicken Sie anschließend auf "Weiter".

7 Klicken Sie im Fenster „Confirm Location“ (Speicherort bestätigen) auf Next (Weiter).

8 Geben Sie im Fenster „Kategorien angeben“ einen Kategorienamen an (z. B. Sentinel), markieren Sie den Namen und klicken Sie auf das Plussymbol.



Hinweis: Nur der erste Bericht wird nach dem Klicken auf „Next“ (Weiter) unter der Kategorie angezeigt.

Klicken Sie anschließend auf "Weiter".

9 Klicken Sie im Fenster „Specify Schedule“ (Zeitplan angeben) auf Let users update the object (Zulassen, dass Benutzer das Objekt aktualisieren) (sollte Standard sein). Klicken Sie anschließend auf "Weiter".

10 Klicken Sie im Fenster „Specify Repository Refresh“ (Repository-Aktualisierung angeben) auf Enable all (Alle aktivieren), um die Repository-Aktualisierung zu aktivieren. Klicken Sie anschließend auf "Weiter".

11 Klicken Sie im Fenster „Specify Keep Saved Data“ (Angabe für das Beibehalten gespeicherter Daten) auf Enable all (Alle aktivieren), um beim Veröffentlichen von Berichten die gespeicherten Daten beizubehalten. Klicken Sie anschließend auf "Weiter".

12 Klicken Sie im Fenster „Change Defaults Values“ (Standardwerte ändern) auf das Optionsfeld Publish reports without modifying properties (Berichte veröffentlichen, ohne Eigenschaften zu ändern) (sollte Standard sein). Klicken Sie anschließend auf "Weiter".

13 Klicken Sie auf Next (Weiter), um Ihre Objekte hinzuzufügen.

14 Klicken Sie anschließend auf "Weiter". Klicken Sie auf Fertig stellen.

Wenn Sie die Sentinel-Schablonen für Crystal Reports im Crystal Reports Server veröffentlichen, müssen sich die Schablonen im Verzeichnis „SentinelReports“ befinden. Anderenfalls werden sie nicht im Sentinel Control Center angezeigt.

9.3.3 Veröffentlichen von Reports-Schablonen – Central Management Console

Sentinel-Berichte werden jetzt mithilfe von Lösungspaketen ausgeliefert. Sie können diese Methode aber auch zum Veröffentlichen von Berichtsschablonen verwenden, die nicht aus einem Lösungspaket stammen.

So importieren Sie Crystal Reports-Schablonen:

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise115/adminlaunch`
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Melden Sie sich bei Crystal Reports Server an.
4. Klicken Sie im Fenster „Organize“ (Organisieren) auf Folders (Ordner).
5. Klicken Sie in der rechten oberen Ecke auf „New Folder“ (Neuer Ordner).
6. Erstellen Sie einen Ordner „SentinelReports“, falls er nicht bereits vorhanden ist. Klicken Sie auf "OK".

   Hinweis: Beim Namen des Ordners gab es keinerlei Abweichung von „SentinelReports“ geben.

   ---
7. Klicken Sie auf „SentinelReports“ (SentinelReports).
8. Klicken Sie auf die Registerkarte „Unterordner“ und erstellen Sie entsprechend Ihren Anforderungen Unterordner. Wenn Sie die Sentinel Core-Berichte manuell hinzufügen, erstellen Sie die folgenden Unterordner:
   - Advisor_Vulnerability
   - Dashboards
   - Incident Management
   - Internal Events
   - Security Events
   - Top 10
9. Wählen Sie die Optionsfolge „Home“ > „Objects“ > „New Object“ (Anfang > Objekte > Neues Objekt).
10. Markieren Sie auf der linken Seite den Eintrag „Report“ (Bericht).
11. Klicken Sie auf „Durchsuchen“ und navigieren Sie zum Verzeichnis der hinzuzufügenden Berichtsschablonen. Wählen Sie einen Ordner und darin einen Bericht aus.
12. Markieren Sie „SentinelReports“ und klicken Sie auf „Unterordner anzeigen“.
13. Wählen Sie den entsprechenden Ordner für den Bericht aus und klicken Sie auf Show Subfolders (Unterordner anzeigen).
14. Klicken Sie auf „Senden“.
15. Wenn Sie die restlichen Berichte hinzufügen möchten, wiederholen Sie Schritt 9 bis 17 so lange, bis alle Berichte hinzugefügt wurden.

9.4 Verwenden von Crystal XI R2 Web Server

Crystal Reports Server XI unter Linux installiert einen Webserver, über den Sie Verwaltungsaufgaben durchführen sowie Berichte veröffentlichen und anzeigen können.

Das Verwaltungsportal kann unter folgender URL über den Browser aufgerufen werden:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

Das nicht für die Verwaltung bestimmte (allgemeine) Portal kann unter folgender URL über den Browser aufgerufen werden:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115
```

9.4.1 Testen der Konnektivität zum Webserver

So testen Sie die Konnektivität zum Webserver:

1. Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.
2. Geben Sie Folgendes an:

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```

   Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

9.4.2 Festlegen eines Kontos für einen benannten Benutzer

Der im Lieferumfang von Crystal Reports Server enthaltene Schlüssel ist ein Kontoschlüssel für „Named User“ (Benannter Benutzer). Das Gastkonto muss von „Concurrent User“ (Gleichzeitiger Benutzer) in „Named User“ (Benannter Benutzer) geändert werden.

So definieren Sie das Gastkonto als „Named User“ (Benannter Benutzer):

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```

2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Klicken Sie im Fenster „Organize“ (Organisieren) auf „Users“ (Benutzer) > „Guest“ (Gast).
5. Ändern Sie den Verbindungstyp von „Concurrent User“ (Gleichzeitiger Benutzer) in „Named User“ (Benannter Benutzer). Klicken Sie auf „Update“ (Aktualisieren).

   Melden Sie sich ab und schließen Sie das Fenster.

9.4.3 Konfigurieren von Berichtsberechtigungen

Hier wird erläutert, wie Sie mit Administration Launchpad die Berechtigungen für Berichte so konfigurieren können, dass Sie in der Lage sind, Berichte nach Bedarf anzuzeigen und zu bearbeiten.

So konfigurieren Sie Berichtsberechtigungen:

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise115/adminlaunch`
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).

   Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf „Log On“ (Anmelden).
4. Klicken Sie im Bereich „Organize“ (Organisieren) auf „Folders“ (Ordner).
5. Führen Sie einen einfachen Mausklick auf „SentinelReports“ aus. Wählen Sie „All“ (Alles).
6. Klicken Sie auf den Karteireiter Rights (Rechte).
7. Wählen Sie im Dropdown-Menü für „Everyone“ (Alle) die Option View on Demand (Auf Verlangen anzeigen) aus.
8. Klicken Sie auf „Update“ (Aktualisieren). Melden Sie sich ab und schließen Sie das Fenster.

9.5 Heraufsetzen der Crystal Reports Server-Grenze für die Berichtsaktualisierung

Wenn Crystal versucht, eine extrem große Anzahl an Ereignissen zu verarbeiten, wird möglicherweise eine Fehlermeldung in Bezug auf die maximale Verarbeitungszeit oder die maximale Anzahl an Datensätzen ausgegegeben. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren.

So konfigurieren Sie Crystal Page Server neu:

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise115/adminlaunch`
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf „Log On“ (Anmelden).
5. Klicken Sie auf „Servers“ (Server); klicken Sie auf „<servername>.pageserver“.
6. Klicken Sie unter „Database Records to Read When Previewing Or Refreshing a report“ (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf „Unlimited records“ (Unbegrenzt viele Datensätze); klicken Sie auf „Apply“ (Anwenden).
7. Sie werden aufgefordert, Page Server neu zu starten. Klicken Sie auf „OK“.
8. Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager des Betriebssystems aufgefordert.

9.6 Konfigurieren von Sentinel Control Center zur Integration in Crystal Reports Server

Sentinel Control Center kann zur Integration in Crystal Reports Server konfiguriert werden, Sie können dann also Crystal Reports in Sentinel Control Center anzeigen.

Gehen Sie zur Integration von Sentinel Control Center in Crystal Reports Server wie nachfolgend beschrieben vor.

Hinweis: Diese Konfiguration darf erst durchgeführt werden, nachdem Crystal Reports Server installiert und Crystal Reports in dieser Anwendung veröffentlicht wurden. Weitere Informationen zu unterstützten Plattformen für Crystal Reports Server in einer Sentinel-Umgebung erhalten Sie unter Kapitel 2, „Systemanforderungen“, auf Seite 21.

So konfigurieren Sie Sentinel für die Integration in Crystal Reports Server:

1. Melden Sie sich bei Sentinel Control Center als Benutzer mit Rechten für die Registerkarte „Admin“ an.
2. Wählen Sie auf der Registerkarte „Admin“ die Option „Konfiguration für Crystal-Bericht“.
3. Geben Sie in das Feld „Analyse-URL“ Folgendes ein:

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   esec-script/
   GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
   ```

   Hinweis: <hostname_oder_IP_von_webserver> muss durch die IP-Adresse bzw. den Hostnamen von Crystal Reports Server ersetzt werden.

   Hinweis: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS die IP-Adresse angegeben ist. Es muss sich um den Hostnamen handeln.

   Hinweis: <web_server_port_default_8080> muss durch den Port ersetzt werden, den der Crystal-Webserver überwacht.

   ---
4. Klicken Sie neben dem Feld „Analyse-URL“ auf Aktualisieren.
5. Wenn Advisor auf Ihrem Computer installiert ist, geben Sie Folgendes in das Feld „Advisor-URL“ ein:

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   esec-script/
   GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
   ```

   Hinweis: <hostname_or_IP_of_web_server> muss durch die IP-Adresse bzw. den Hostnamen von Crystal Reports Server ersetzt werden.

   Hinweis: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS die IP-Adresse angegeben ist. Es muss sich um den Hostnamen handeln.

Hinweis: <web_server_port_default_8080> muss durch den Port ersetzt werden, den der Crystal-Webserver überwacht.

6 Klicken Sie neben dem Feld „Advisor URL“ auf Aktualisieren;

Klicken Sie auf "Speichern".

7 Melden Sie sich beim Sentinel Control Center ab und erneut wieder an.

Die Crystal Reports-Bäume auf den Registerkarten „Analyse“ und „Advisor“ (wenn Advisor installiert ist), sollten nun im Navigatorfenster angezeigt werden.

9.7 Dienstprogramme und Fehlersuche

9.7.1 Starten von MySQL

So vergewissern Sie sich, dass MySQL ausgeführt wird:

1 Melden Sie sich als Crystal-Benutzer an.

2 Wechseln Sie zu „/opt/crystal_xir2/bobje“

3 `./mysqlstartup.sh`

9.7.2 Starten von Tomcat

So vergewissern Sie sich, dass Tomcat ausgeführt wird:

1 Melden Sie sich als Crystal-Benutzer an

2 Wechseln Sie zu „/opt/crystal_xir2/bobje“

3 `./tomcatstartup.sh`

9.7.3 Starten von Crystal Reports Server-Instanzen

So stellen Sie sicher, dass Crystal Reports Server-Instanzen ausgeführt werden:

1 Melden Sie sich als Crystal-Benutzer an

2 Wechseln Sie zu „/opt/crystal_xir2/bobje“

3 `./startservers`

9.7.4 Fehler beim Crystal-Hostnamen

So lösen Sie einen Fehler beim Hostnamen auf:

1 Wenn Sie folgende Fehlermeldung erhalten:

```
Warning: ORB::BOA_init: hostname lookup returned `localhost'
(127.0.0.1)
Use the -OAhost option to select some other hostname
```

Vergewissern Sie sich, dass Ihre IP-Adresse und Ihr Hostname sich in der Datei /etc/hosts befinden. Beispiel:

```
10.0.0.1   linuxCE02
```

9.7.5 Verbindung mit CMS nicht möglich

Wenn das System meldet, dass es keine Verbindung zu CMS herstellen kann, versuchen Sie das Problem durch Ausführung folgender Befehle zu lösen.

So führen Sie eine Fehlersuche bei Problemen mit der CMS-Verbindung durch:

1 Wenn der Befehl „netstat –an | grep 6400“ zu keinem Ergebnis führt, versuchen Sie folgende Vorgehensweise:

- Geben Sie die MySQL-Verbindungsinformationen erneut ein:
  1. Melden Sie sich als Crystal-Benutzer an
  2. Wechseln Sie zu „/opt/crystal_xir2/bobje“
  3. `./cmsdbsetup.sh`
  4. Drücken Sie die Eingabetaste wenn `[<hostname>.cms]` angezeigt wird.
  5. Wählen Sie alle während der Installation eingegebenen Informationen zur MySQL-Datenbank aus bzw. geben Sie sie an. Weitere Informationen finden Sie in den Installationsanweisungen in Kapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31.
  6. Beenden Sie abschließend `cmsdbsetup.sh`
  7. `./stopservers`
  8. `./startservers`
- Initialisieren Sie die MySQL-Datenbank neu:
  1. Melden Sie sich als Crystal-Benutzer an
  2. Wechseln Sie zu „/opt/crystal_xir2/bobje“
  3. `./cmsdbsetup.sh`
  4. Drücken Sie die Eingabetaste wenn `[<hostname>.cms]` angezeigt wird.
  5. Wählen Sie „Reinitialize“ (Neu initialisieren) und befolgen Sie die Anweisungen.
  6. Beenden Sie abschließend `cmsdbsetup.sh`
  7. `./stopservers`
  8. `./startservers`

1 Vergewissern Sie sich, dass alle CCM-Server aktiviert sind:

1a Melden Sie sich als Crystal-Benutzer an

1b Wechseln Sie zu „/opt/crystal_xir2/bobje“

1c `./ccm.sh` -enable all

9.8 Auf Hochleistung ausgerichtete Konfigurationen für Crystal

Je nachdem, wie viele Ereignisse Crystal abfragt, erhalten Sie möglicherweise eine Fehlermeldung bezüglich der maximalen Verarbeitungszeit oder der maximalen Datensatzgrenze. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren. Dieser Vorgang kann entweder über Central Configuration Manager oder über die Crystal-Webseite durchgeführt werden.

So konfigurieren Sie Crystal Page Server über Central Configuration Manager neu:

1. Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und wählen Sie „Stopp“.
3. Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ und wählen Sie „Properties“ (Eigenschaften).
4. Fügen Sie auf dem Karteireiter „Properties“ (Eigenschaften) im Feld „Command“ (Befehl) am Ende der Befehlszeile Folgendes hinzu:

   ```
   maxDBResultRecords <value greater than 20000 or 0 to disable the
   default limit>
   ```

5. Starten Sie Crystal Page Server neu.

So konfigurieren Sie Crystal Page Server über die Central-Verwaltungskonsole neu:

1. Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects 11“ > „Crystal Reports Server“ > „.NET Administration Launchpad“. Sie können auch einen Webbrowser öffnen und die folgende URL eingeben:

   http://<DNS-Name oder IP-Adresse Ihres Webservers>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort an und klicken Sie auf „Log On“ (Anmelden). Klicken Sie auf Servers (Server).
5. Klicken Sie auf „<server name>.pageserver“.
6. Klicken Sie unter „Database Records to Read When Previewing Or Refreshing a report“ (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf „Unlimited records“ (Unbegrenzt viele Datensätze). Klicken Sie auf "Anwenden".
7. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf „OK“.

Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager des Betriebssystems aufgefordert.

9.8.1 Berichte, die den Aggregierungsdienst verwenden.

Zur Verbesserung der Leistung fragen die 10 wichtigsten im Sentinel Core Solution Pack enthaltenen Berichte Zusammenfassungstabellen anstatt der Ereignistabelle ab. Die Zusammenfassungstabellen enthalten mit der Zeit Zahlen für Kombinationen von Feldern in den Ereignisdaten. Dies bietet einen wesentlich geringeren Datensatz für bestimmte Abfragetypen und führt zu viel schnelleren Abfragen und Berichtslaufzeiten.

Der Aggregationsdienst ist für das Auffüllen der Zusammenfassungstabellen mit Zusammenfassungen der Ereignisse in der Ereignistabelle verantwortlich. Der Aggregationsdienst generiert nur zusammengefasste Daten für Zusammenfassungen, die aktiv sind. Die folgenden Zusammenfassungen werden von den Top 10-Berichten benötigt und sind standardmäßig aktiviert:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Zusammenfassungen können mithilfe des Fensters „Konfiguration der Berichtsdaten“ unter der Registerkarte „Admin“ im Sentinel Control Center aktiviert bzw. deaktiviert werden.

Der Aggregationsdienst ist außerdem von der Komponente `EventFileRedirectService` in DAS Binary abhängig, um ihm die Ereignisdaten bereitzustellen, die es zusammenfasst. Deshalb muss diese Komponente aktiviert werden, damit der Aggregationsdienst ordnungsgemäß ausgeführt wird. Diese Komponente wird durch Ändern des Attributs „status“ der Komponente `EventFileRedirectService` in der Datei `das_binary.xml` aktiviert bzw. deaktiviert. Standardmäßig ist diese Komponente aktiviert.

Hinweis: Informationen zu EventFileRedirectService und den drei Aggregierungszusammenfassungen erhalten Sie in “Konfiguration der Berichtsdaten” in „Admin“ im *Sentinel-Benutzerhandbuch*.

Hinweis: Berichte, die einen großen Datenbereich abfragen, nehmen eventuell einige Zeit in Anspruch. Sie können geplant und nicht interaktiv ausgeführt werden. Informationen zum Einplanen von Crystal-Berichten erhalten Sie in der Dokumentation zu Crystal Reports Server XI R2 (http://support.businessobjects.com/documentation/product_guides/default.asp).

9.8.2 Report Development

Der Crystal Reports Developer kann zum Erstellen oder Ändern von Crystal-Berichten verwendet werden. Für benutzerdefinierte entwickelte Berichte wird Folgendes empfohlen:

- Wenn die Berichte vordefinierte aggregierte Tabellen verwenden können, wählen Sie diejenige aggregierte Tabelle aus, bei der die wenigsten Daten verarbeitet werden.
- Versuchen Sie, einen möglichst großen Teil der Verarbeitung auf die Datenbank-Engine zu verlagern.
- Um den Verarbeitungs-Overhead in Crystal Server zu verringern, sollten Sie die in Crystal Server zu ladende Datenmenge so gering wie möglich halten.
- Schreiben Sie Berichte immer gegen die von Novell bereitgestellten Datenbankansichten und nicht gegen die Basistabellen.

Deinstallieren von Sentinel

10

- Abschnitt 10.1, „Deinstallieren von Sentinel“, auf Seite 147
- Abschnitt 10.2, „Nach der Deinstallation“, auf Seite 149

Zum Entfernen einer Sentinel-Installation werden Deinstallationsprogramme für Linux, Solaris und Windows bereitgestellt. Einige Dateien, einschließlich Protokolldateien, werden beibehalten und können bei Bedarf entfernt werden. Vor dem Durchführen einer neuen Installation wird dringend empfohlen, alle der folgenden Schritte durchzuführen, um sicherzustellen, dass keine Dateien oder Systemeinstellungen einer vorherigen Installation übrig bleiben.

Warnung: Diese Anweisungen beinhalten Änderungen an Betriebssystemeinstellungen und Dateien. Wenn Sie keine Erfahrung im Ändern dieser Systemeinstellungen bzw. Dateien haben, wenden Sie sich an den Systemadministrator.

10.1 Deinstallieren von Sentinel

10.1.1 Deinstallation unter Solaris und Linux

So verwenden Sie das Sentinel-Deinstallationsprogramm für Solaris und Linux:

1. Melden Sie sich als Benutzer „root“ an.
2. Stoppen Sie Sentinel Server.
3. Navigation:
   `$ESEC_HOME/_uninst`
4. Geben Sie Folgendes an:

   Für GUI-Modus:

   `./uninstall.bin`

   Oder

   Für den textbasierten („serielle Konsole“) Modus:

   `./uninstall.bin -console`
5. Wählen Sie eine Sprache aus und klicken Sie auf „OK“.
6. Der Sentinel Install Shield-Assistent wird angezeigt. Klicken Sie anschließend auf "Weiter".
7. Wählen Sie die zu deinstallierenden Komponenten aus und klicken Sie auf „Weiter“.
8. Stellen Sie sicher, dass alle ausgeführten Sentinel-Anwendungen gestoppt sind, und klicken Sie auf „Weiter“.

9 Wenn Sie ausgewählt haben, die Komponente „Datenbank“ zu deinstallieren, werden Sie zum Auswählen einer der folgenden Optionen aufgefordert:

- **Gesamte Datenbankinstanz löschen:** Entfernt die Datenbankinstanz und gibt von der Datenbank verwendeten Speicherplatz frei.
- **Nur die Datenbankobjekte löschen:** Entfernt die Inhalte der Datenbank bis auf den Benutzer „esecdba“. Die Datenbankinstanz kann dann mithilfe des Sentinel-Installationsprogramms erneut aufgefüllt werden. Bei dieser Option wird kein Speicherplatz freigegeben.

10 Wenn Sie „Nur die Datenbankobjekte löschen“ ausgewählt haben, werden Sie zur Eingabe des Passworts für „esecdba“ aufgefordert. Klicken Sie anschließend auf "Weiter".

11 Es wird eine Zusammenfassung der für die Deinstallation ausgewählten Funktionen angezeigt. Klicken Sie auf "Deinstallieren".

12 Klicken Sie auf Fertig stellen.

10.1.2 Deinstallation unter Windows

So verwenden Sie das Sentinel Windows-Deinstallationsprogramm:

1 Melden Sie sich als Administrator an.

2 Stoppen Sie Sentinel Server.

3 Wählen Sie „Start“ > „Alle Programme“ (Windows XP) oder „Programme“ (Windows 2000) > „Sentinel“ > „Sentinel deinstallieren“ aus. Sie können auch „%Esec_home%_uninst“ unter „Start“ > „Ausführen“ eingeben und auf `uninstall.exe` doppelklicken.

4 Wählen Sie eine Sprache aus und klicken Sie auf „OK“.

5 Der InstallShield-Assistent von Sentinel 6.1 wird angezeigt. Klicken Sie anschließend auf "Weiter".

6 Wählen Sie die zu deinstallierenden Komponenten aus und klicken Sie auf „Weiter“.

7 Stellen Sie sicher, dass alle ausgeführten Sentinel-Anwendungen gestoppt sind, und klicken Sie auf „Weiter“.

8 Wenn Sie ausgewählt haben, die Komponente „Datenbank“ zu deinstallieren, werden Sie zum Auswählen einer der folgenden Optionen aufgefordert:

- **Gesamte Datenbank löschen:** Entfernt die Datenbank und gibt von der Datenbank verwendeten Speicherplatz frei.
- **Nur die Datenbankobjekte löschen:** Entfernt die Inhalte der Datenbank bis auf den Benutzer „esecdba“. Die Datenbank kann dann mithilfe des Sentinel-Installationsprogramms erneut aufgefüllt werden. Bei dieser Option wird kein Speicherplatz freigegeben.

9 Wenn Sie ausgewählt haben, die Komponente „Datenbank“ zu deinstallieren, werden Sie zum Auswählen einer der folgenden Optionen aufgefordert:

- **Windows-Authentifizierung:** Zum Verwenden der Windows-Authentifizierung müssen Sie bei Windows als MS SQL Server-Instanz-Systemadministrator angemeldet sein.
- **SQL-Authentifizierung:** Geben Sie Benutzernamen und Passwort dieses Systemadministrators (oder vergleichbares) an.

Klicken Sie anschließend auf "Weiter".

10 Es wird eine Zusammenfassung der für die Deinstallation ausgewählten Funktionen angezeigt. Klicken Sie auf "Deinstallieren".

11 Wählen Sie das Neubooten des Systems aus und klicken Sie auf „Fertig stellen“.

10.2 Nach der Deinstallation

10.2.1 Sentinel-Einstellungen

Nach der Deinstallation von Sentinel bleiben einige Systemeinstellungen vorhanden, die manuell entfernt werden können. Diese Einstellungen sollten entfernt werden, bevor eine „saubere“ Installation von Sentinel ausgeführt wird, insbesondere dann, wenn bei der Deinstallation von Sentinel Fehler aufgetreten sind.

Hinweis: Bei Solaris und Linux wird durch das Deinstallieren von Sentinel Server der Sentinel-Administratorbenutzer nicht aus dem Betriebssystem entfernt. Sie müssen diesen Benutzer bei Bedarf manuell entfernen.

Entfernen der Sentinel-Systemeinstellungen unter Linux

So bereinigen Sie Sentinel unter Linux manuell:

1 Melden Sie sich als „root“ an.

2 Stellen Sie sicher, dass alle Sentinel-Prozesse gestoppt sind.

3 Entfernen Sie die Inhalte von „/opt/novell/sentinel6“ (bzw. dem Verzeichnis, in dem die Sentinel-Software installiert wurde).

4 Entfernen Sie die Startdateien des Sentinel-Diensts:

Auf SLES:

```
chkconfig --del sentinel
```

Unter RedHat:

```
rm /etc/rc.d/rc0.d/K02sentinel
rm /etc/rc.d/rc3.d/S98sentinel
rm /etc/rc.d/rc5.d/S98sentinel
```

5 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/rc.d/rc0.d`, falls vorhanden:

- K01wizard
- K01esdee
- K01esyslogserver

6 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/rc.d/rc3.d`, falls vorhanden:

- S99wizard
- S99esyslogserver
- S99esdee

7 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/rc.d/rc5.d`, falls vorhanden:

- S99wizard

- S99esyslogserver
- S99esdee

8 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/init.d`, falls vorhanden:

- sentinel
- wizard
- esdee
- esyslogserver

9 Stellen Sie sicher, dass niemand als Sentinel-Administrator-Systembenutzer angemeldet ist (standardmäßig „esecadm“) und entfernen Sie dann den Benutzer (und das Basisverzeichnis) sowie die Gruppe „esec“.

- Führen Sie Folgendes aus: `userdel -r esecadm`.
- Führen Sie Folgendes aus: `groupdel esec`.

10 Entfernen Sie das Verzeichnis /root/InstallShield

11 Entfernen Sie die Datei /root/vpd.properties

12 Entfernen Sie den InstallShield-Abschnitt von `/etc/profile und /etc/.login`.

13 Entfernen Sie die Sentinel Oracle-Datenbank. Weitere Informationen finden Sie unter „Entfernen der Sentinel Oracle-Datenbank unter Linux und Solaris“ auf Seite 151.

14 Starten Sie das Betriebssystem neu.

Entfernen der Sentinel-Systemeinstellungen unter Solaris

So bereinigen Sie Sentinel unter Solaris manuell :

1 Melden Sie sich als „root“ an.

2 Stellen Sie sicher, dass keine Sentinel-Prozesse ausgeführt werden.

3 Entfernen Sie die Inhalte von `/opt/novell/sentinel6` (bzw. dem Verzeichnis, in dem die Sentinel-Software installiert wurde).

4 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/rc0.d`, falls vorhanden:

- K01wizard
- K02sentinel
- K01esdee
- K01esyslogserver

5 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/rc3.d` , falls vorhanden:

- S98sentinel
- S99wizard
- S99esyslogserver
- S99esdee

6 Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/init.d`, falls vorhanden:

- sentinel
- wizard

- esdee
- esyslogserver

7 Entfernen Sie die folgenden Dateien im Verzeichnis `/usr/local/bin`, falls vorhanden:

- `stop_wizard.sh`
- `restart_wizard.sh`
- `start_wizard.sh`

8 Stellen Sie sicher, dass niemand als Sentinel-Administrator-Systembenutzer angemeldet ist (standardmäßig „esecadm“) und entfernen Sie dann den Benutzer (und das Basisverzeichnis) sowie die Gruppe „esec“.

- Führen Sie Folgendes aus: `userdel -r esecadm`.
- Führen Sie Folgendes aus: `groupdel esec`.

9 Entfernen Sie den InstallShield-Abschnitt von `/etc/profile and /etc/.`Anmeldung

10 Entfernen Sie das Verzeichnis /InstallShield, sofern vorhanden.

11 Bereinigen Sie die InstallShield-Verweise in `/var/sadm/pkg.` Wenn die folgenden Dateien vorhanden sind. Entfernen Sie die folgenden Dateien aus dem Verzeichnis `/var/sadm/pkg` :

- Alle Dateien, die mit IS beginnen (IS* in der Befehlszeile)
- Alle Dateien, die mit ES beginnen (ES* in der Befehlszeile)
- Alle Dateien, die mit MISCwp beginnen (MISCwp* in der Befehlszeile)

12 Entfernen Sie die Sentinel Oracle-Datenbank. Weitere Informationen finden Sie unter „Entfernen der Sentinel Oracle-Datenbank unter Linux und Solaris“ auf Seite 151.

13 Starten Sie das Betriebssystem neu.

Entfernen der Sentinel Oracle-Datenbank unter Linux und Solaris

So bereinigen Sie die Sentinel Oracle-Datenbank unter Linux und Solaris manuell:

Hinweis: Stellen Sie sicher, dass keine anderen Anwendungen diese Datenbank verwenden, bevor Sie sie entfernen.

---

1 Melden Sie sich als „oracle“ an.

2 Stoppen Sie den Oracle Listener:

- Führen Sie Folgendes aus: `lsnrctl stop`.

3 Stoppen Sie die Sentinel-Datenbank:

- Setzen Sie die Umgebungsvariable ORACLE_SID auf den Namen Ihrer Sentinel-Datenbankinstanz (standardmäßig ESEC).
- Führen Sie Folgendes aus: `sqlplus "/ as sysdba"`.
- Führen Sie an der sqlplus-Eingabeaufforderung Folgendes aus: `shutdown immediate`.

4 Entfernen Sie den Eintrag für die Sentinel-Datenbank in der Datei „oratab“, die sich hier befindet:

Unter Linux:

`/etc/oratab`

Unter Solaris:

`/var/opt/oracle/oratab`

5 Entfernen Sie die Datei „init<Ihr_Instanz_Name>.ora (Standard `initESEC.ora`) aus dem Verzeichnis „$ORACLE_HOME/dbs“.

6 Entfernen Sie die Einträge für Ihre Sentinel-Datenbank aus folgenden Dateien im Verzeichnis $ORACLE_HOME/network/admin:

- `tnsnames.ora`
- `listener.ora`

7 Löschen Sie die Datendateien der Datenbank aus dem Verzeichnis, in dem Sie sie installiert haben.

8 Löschen Sie die Archivdateien der Datenbank aus dem Verzeichnis, in dem Sie sie erstellt haben.

Entfernen Sie die Sentinel-Systemeinstellungen von Windows mit MS SQL Server.

So bereinigen Sie Sentinel unter Windows manuell :

1 Löschen Sie den Ordner „%CommonProgramFiles%\InstallShield\Universal“ und alle darin enthaltenen Inhalte.

2 Löschen Sie den Ordner „%ESEC_HOME%“ (standardmäßig unter „C:\Programme\Novell\Sentinel6“).

3 Klicken Sie mit der rechten Maustaste auf „Arbeitsplatz“ > „Eigenschaften“ > „Erweitert“.

4 Klicken Sie auf die Schaltfläche "Umgebungsvariablen".

5 Löschen Sie die folgenden Variablen, sofern vorhanden:

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

6 Entfernen Sie alle Einträge in der Umgebungsvariable „PATH“, die auf die Sentinel-Installation verweisen.

Warnung: Entfernen Sie keine Pfade zu anderen Speicherorten als zu der alten Sentinel-Installation. Dies könnte dazu führen, dass Ihr System nicht ordnungsgemäß funktioniert.

---

7 Löschen Sie alle Sentinel-Verknüpfungen vom Desktop.

8 Löschen Sie den Verknüpfungsordner „Start“ > „Programme“ > „Sentinel“ aus dem Startmenü.

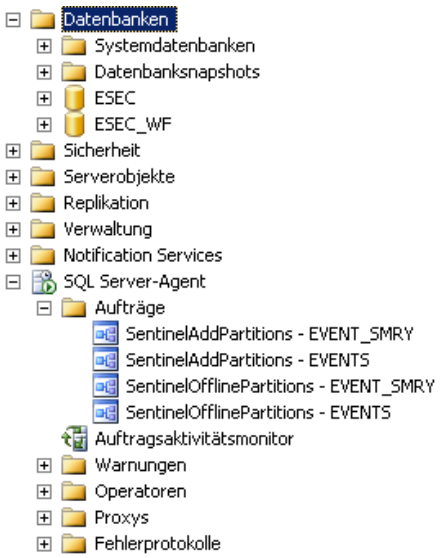
9 Starten Sie das Betriebssystem neu.

So bereinigen Sie die Sentinel Microsoft SQL Server-Datenbank unter Windows manuell :

Hinweis: Stellen Sie sicher, dass keine anderen Anwendungen diese Datenbank verwenden, bevor Sie sie entfernen.

---

1 Öffnen Sie Microsoft SQL Server Management Studio und stellen Sie eine Verbindung zu der SQL Server-Instanz her, auf der Sie Ihre Sentinel-Datenbank installiert haben.



2 Erweitern Sie den Baum „SQL Server-Agent“ > „Aufträge“ und entfernen Sie die Sentinel-Aufträge.

3 Erweitern Sie den Baum „Datenbank“ und suchen Sie die Sentinel-Datenbank. Es sollte eine Sentinel-Datenbank (standardmäßig mit Namen „ESEC“) und eine iTRAC-Datenbank (standardmäßig mit Namen „ESEC_WF“) vorhanden sein. Klicken Sie jeweils mit der rechten Maustaste darauf und wählen Sie „Löschen“ aus.

4 Bestätigen Sie das Löschen der Datenbank mit Ja.

5 Erweitern Sie den Baum „Sicherheit“ > „Anmelden“ und entfernen Sie die Sentinel-Datenbankbenutzer, sofern diese vorhanden sind.

- Esecdba
- Esecapp
- Esecadm
- Esecrpt

6 Löschen Sie die Archivdateien der Datenbank aus dem Verzeichnis, in dem Sie sie erstellt haben.

Fragebogen vor der Installation

A

Die Beantwortung der folgenden Fragen kann beim Planen Ihrer eigenen Installation hilfreich sein, oder wenn Sie sich darauf vorbereiten, dass Berater Ihr Sentinel-System installieren.

Fragen vor der Installation

1 Zu welchem Zweck bzw. mit welchem Ziel verwenden Sie Novell Sentinel?

   1a Einhaltung von Bestimmungen

   1b Verwaltung von Sicherheitsereignissen

   1c Sonstiges_____

2 Welche Hardware wurde für die Installation von Sentinel zugeordnet? Ist dies in Zusammenhang mit Hardwarespezifikationen, die in der Sentinel-Installationsanleitung angegeben sind?

3 Haben Sie die Anforderungen an Hardware und Betriebssystem von Sentinel, die in der Sentinel-Installationsanleitung beschrieben sind, hinsichtlich Ihrer Konfiguration überprüft?

   - Betriebssystem-Patch-Stufe
   - Service-Patches
   - Hot Fixes usw.

4 Erfüllt Ihr DAS-Computer die erforderlichen Betriebssystem- und Hardwareanforderungen?

5 Welche Netzwerkarchitektur verwenden die Quellgeräte hinsichtlich des Sicherheitssegments, in dem sich die Sentinel-/Collector-Hardware befinden soll?

Hinweis: Dies ist zum Verständnis der Hierarchie der Collector-Datensammlung wichtig und zum Identifizieren von Firewalls, die penetriert werden müssen, um die Kommunikation von Collector zu Sentinel, von Sentinel zur Datenbank oder von Crystal Server zur Datenbank zu ermöglichen.

Geben Sie unten Informationen (Text und/oder Zeichnung) bzw. einen Link zu Informationen an.

6 Welche Berichte sollen über das System erstellt werden? Dies ist wichtig, um sicherzustellen, dass die Collectors die richtigen Daten für die Weitergabe an die Sentinel-Datenbank sammeln.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 Aus welchen Quellgeräten möchten Sie Daten sammeln (IDS, HIDS, Router, Firewalls, usw.), Ereignisrate (EPS – Ereignisse pro Sekunde), Versionen, Verbindungsmethoden, Plattformen und Patches?

Gerät (Hersteller/ Modell)	Ereignisrate (EPS)	Version	Verbindungsmethode	Plattform	Patches

Können Sie Beispiele für Daten angeben, die die Sentinel Collectors sammeln und analysieren sollen? Sentinel kann so konfiguriert werden, dass die gewünschte Ausgabe auf Grundlage der hier angegebenen Informationen bereitgestellt werden kann.

8 Welche Sicherheitsmodelle/Standards sind an Ihrem Standort vorhanden?

- Wie ist Ihre Haltung in Bezug auf lokale Konten gegenüber Domänenauthentifizierung?
  - Für Windows mit Domänenauthentifizierung müssen die richtigen Domänenkontoeinstellungen erstellt werden, damit Sentinel installiert werden kann.
  - Für die Solaris-Installation gilt dies nicht. Sentinel unterstützt jedoch nicht NIS.

9 Wie lange müssen die Daten beibehalten werden (in Tagen)?

10 Welche Datenträgergröße möchten Sie auf der Grundlage der Informationen über die Datenbeibehaltung und EPS verwenden? Verwenden Sie 500 bis 800 Byte/Ereignis für Größenschätzungen.

11 Welche Ereignismuster sollen in Ihren Daten identifiziert werden?

12 Unterstützen die aktuellen Daten Ihrer Ereignisquellen die Ereignismuster, die erkannt werden sollen, oder wird eine Ereignisanreicherung mithilfe des Zuordnungsdiensts benötigt?

13 Wenn der Zuordnungsdienst benötigt wird, was ist die Quelle der Anreicherungsdaten und welcher Schlüssel wird für die Zuordnung verwendet? Wie werden die Zuordnungen auf dem neuesten Stand gehalten?

14 Wenn eine Gefährdung der Sicherheit oder der Kompatibilität erkannt wird, welche Prozesse werden für die Korrektur verwendet?

Oracle-Setup

B

B.1 Installation von Oracle

Wichtig: HAFTUNGSAUSSCHLUSS: Die in diesem Dokument bereitgestellten Anweisungen beabsichtigen nicht die Dokumentation von Oracle zu ersetzen. Es handelt sich hierbei nur um ein Beispiel eines Einrichtungsszenarios. Diese Dokumentation setzt voraus, dass das Basisverzeichnis des Oracle-Benutzers „//home/oracle“ lautet und dass Oracle im Verzeichnis „/opt/oracle“ installiert wird. Ihre genaue Konfiguration ist eventuell anders. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem und zu Oracle.

Weitere Informationen zu Oracle-Installationen und zum korrekten Patch-Level, der für Sentinel zertifiziert oder unterstützt wird, erhalten Sie im Abschnitt Kapitel 2, „Systemanforderungen“, auf Seite 21.

B.1.1 Oracle 10g-Installation auf SLES 10

So installieren Sie Oracle auf SUSE Linux Enterprise Server 10:

1. Befolgen Sie die im SLES 10-Installationshandbuch bereitgestellten Installationsanweisungen. Installieren Sie SLES 10 mit dem Dateisystem „ext3“ und den Standardpaketen zusammen mitOracle Server Base, C/C++ Compiler und Tools.
2. Melden Sie sich als „root“ an.
3. Installieren Sie das Servicepack SLES 10. Überprüfen Sie die Service Pack-Informationen, indem Sie Folgendes eingeben:

   ```
   SPident
   ```

   oder

   ```
   cat /etc/SuSE-release
   ```

   Zum Zeitpunkt dieser Dokumentation wurde das SLES 10-Service-Pack noch nicht veröffentlicht. Verwenden Sie zur Überprüfung „SPident“ oder „cat/etc/SUSE-release“.

   Folgendes sollte angezeigt werden:

   ```
   CONCLUSION: System is up-to-date!
     Found     SLES-10-x86_64-current
   ```
4. Das Konto für den Oracle-Benutzer ist deaktiviert. Aktivieren Sie es, indem Sie die Shell für den Oracle-Benutzer mit der YaST-Benutzerverwaltung von „/bin/false“ in „/bin/bash“ ändern bzw. indem Sie die Datei „/etc/passwd“ bearbeiten.
5. Legen Sie ein neues Passwort für den Oracle-Benutzer fest, indem Sie YaST verwenden oder Folgendes eingeben:

   ```
   /usr/bin/passwd oracle
   ```

6 Ändern Sie den standardmäßigen Oracle-Umgebungssatz gegebenenfalls durch „orarun“:

- Ändern Sie das Oracle-Basisverzeichnis durch Bearbeiten der ORACLE_HOME-Variable in der Datei `/etc/profile.d/oracle.sh`.
- Der standardmäßige ORACLE_SID-Satz der orarun-Installation ist „orcl“. Ändern Sie ihn in der Datei `/etc/profile.d/oracle.sh` in ESEC.

7 Führen Sie zum Festlegen der Kernel-Parameter Folgendes aus:

```
/usr/sbin/rcoracle start
```

8 Wechseln Sie zum Benutzer „oracle“

```
su - oracle
```

9 Wechseln Sie in das Datenbankverzeichnis und führen Sie Folgendes aus: `./runinstaller` (Oracle Universal Installer). Ein Fehler wie unten gezeigt wird angezeigt:

10 Beheben Sie den Fehler, indem Sie eine der folgenden Optionen ausführen:

- Ändern Sie die Datei `database/install/oraparam.ini`, um Unterstützung für SUSE Linux 10 hinzuzufügen. Nach dem Ändern der Datei „oraparam.ini“ „[Zertifizierte Versionen]“ sieht die Zeile wie folgt aus:

  ```
  [Certified Versions]
  Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
  ```

- Installation mit der Option „-ignoreSysPrereqs“

  ```
  that is ./runInstaller –ignoreSysPrereqs
  ```

11 Akzeptieren Sie das standardmäßige Inventarverzeichnis oder suchen Sie ein neues Verzeichnis. Klicken Sie anschließend auf "Weiter".

12 Wählen Sie aus den Installationstypen „Enterprise Edition“ aus. Klicken Sie anschließend auf "Weiter".

13 Wählen Sie zum Überprüfen der Netzwerkkonfigurationsanforderungen „User Verified“ (durch Benutzer geprüft) aus. Klicken Sie anschließend auf "Weiter".

14 Wählen Sie aus den Konfigurationsoptionen „Nur Datenbanksoftware installieren“ aus. Klicken Sie anschließend auf "Weiter".

15 Die Installationszusammenfassung wird angezeigt. Überprüfen Sie sie und klicken Sie auf „Installieren“.

16 Führen Sie die angegebenen Skripts als Stamm aus und klicken Sie nach dem Abschluss auf „OK“.

17 Klicken Sie nach der Installation auf „Beenden“.

B.1.2 Oracle 10g Installation auf Red Hat Linux 4

So installieren Sie Oracle auf Red Hat Linux:

1 Melden Sie sich als Root an.

2 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die erforderlichen Pakete (unten aufgeführt) auf Ihrem Server installiert sind.

```
rpm –q make
```

Liste mit Paketen:

```
compat –db
compat-gcc-32
compat-gcc-32-c++
compat-oracle-rhel4
compat-libcwait
compat-libgcc-296
compat-libstdc++-296
compat-libstdc++-33
gcc
gcc-c++
gnome-libs
gnome-libs-devel
libaio-devel
libaio
make
openmotif21
xorg-x11-deprecated-libs-devel
xorg-x11-deprecated-libs
```

3 Erstellen Sie eine UNIX-Gruppe und ein UNIX-Benutzerkonto für den Oracle-Datenbankeigentümer.

Fügen Sie eine dba-Gruppe hinzu (als „root“):

```
groupadd oinstall
groupadd dba
```

4 Fügen Sie den Oracle-Benutzer hinzu (als „root“):

```
useradd –g oinstall –G dba –d /opt/oracle/product/<10.2.0.3>/db_1 –
m oracle
passwd oracle
```

5 Erstellen Sie ein Verzeichnis für ORACLE_HOME und ORACLE_BASE:

```
mkdir –p /opt/oracle/product/<10.2.0.3>
```

6 Ändern Sie die Eigentümereinstellungen des Verzeichnisses ORACLE_BASE und darunter bis „oracle/oinstall“:

```
chown -R oracle:oinstall /opt/oracle
```

7 Wechseln Sie zum Benutzer „oracle“

```
su - oracle
```

8 Öffnen Sie die Datei `.bash_profile` (im Basisverzeichnis des Benutzers „oracle“) und fügen Sie Folgendes an das Dateiende an:

Hinweis: Diese Umgebungsvariablen dürfen nur für den Benutzer „oracle“ verwendet werden. Sie sollten keinesfalls in der Systemumgebung oder in der Umgebung des Sentinel-Administrators festgelegt werden.

```
# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/JRE:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/
jlib
```

```
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEl=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP;export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME
```

9 Speichern Sie die Datei `.bash_prolie` und beenden Sie den Vorgang.

10 Melden Sie sich erneut als Benutzer „oracle“ an, um die Änderungen der Umgebungsvariablen im letzten Schritt zu laden:

```
exit
su - oracle
```

11 Überprüfen Sie mithilfe des folgenden Befehls, ob `.bash_profile` wie erwartet ausgeführt wurde:

```
set | more
```

12 Melden Sie sich als Oracle-Benutzer and. Wenn Sie X-Emulation verwenden, legen Sie die DISPLAY-Umgebungsvariable fest:

```
DISPLAY=<machine-name>:0.0; export DISPLAY
```

13 Wenn Sie Oracle 10.2.0.1 von der Disk1 installieren möchten, führen Sie folgendes Skript aus:

```
./runInstaller
```

14 Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.

- Klicken Sie im Fenster „Willkommen“ auf „Weiter“.
- Wählen Sie im Fenster „Dateispeicherort“ aus dem Dropdown-Menü „OUIHome“ aus. Klicken Sie anschließend auf "Weiter".
- Wählen Sie im Fenster „Product to Install“ (Zu installierendes Produkt) je nach Ihrer Version „Oracle 10g Datenbank“ 10.2.0.1 aus. Klicken Sie auf „Weiter“.
- Wählen Sie im Fenster „Installationstypen“ die Option „Enterprise Edition“ aus. Klicken Sie anschließend auf "Weiter".
- Wählen Sie im Fenster „Datenbankkonfiguration“ die Option „General Purpose“ (Allgemein) aus. Klicken Sie anschließend auf "Weiter".
- Überprüfen Sie im Fenster „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf „Installieren“.
- Am Ende des Installationsfensters klicken Sie auf „Beenden“.

15 Zum Anwenden des Oracle 10.2.0.3 Patch auf der Disk1 der Oracle 10.2.0.3 Patch-Distribution führen Sie das Skript aus:

```
./runInstaller
```

16 Befolgen Sie die Eingabeaufforderungen in den Installationsfenstern. Überprüfen Sie im Fenster „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf „Installieren“. Am Ende des Installationsfensters klicken Sie auf „Beenden“.

B.1.3 Oracle 10g Installation auf Solaris 10

Hinweis: Weitere Informationen zu den Prozeduren zum Definieren der Kernelparametereinstellungen in Solaris 10 erhalten Sie in Abschnitt 3.4.1, „Festlegen von Kernel-Werten“, auf Seite 40.

So installieren Sie Oracle 10g auf Solaris 10:

1. Melden Sie sich als Root an.
2. Starten Sie die Installation

```
#  su - oracle
# < Installation directory or CD mount>/ .runInstaller
```

3. Im Fenster „Willkommen“:
   - Wählen Sie die einfache Installation aus.
   - Deaktivieren Sie das Kontrollkästchen „Create Starter Database“ (Startdatenbank erstellen).
   - Geben Sie den Oracle-Basisspeicherort an.
   - Die UNIX DBA-Gruppe ist üblicherweise „dba“. Klicken Sie anschließend auf "Weiter".
4. Im Fenster „Product-Specific Prerequisite“ (Produktspezifische Voraussetzungen):
   - Überprüfen Sie, ob alle Systemüberprüfungen erfolgreich waren. Klicken Sie anschließend auf "Weiter".
5. Im Fenster „Zusammenfassung“:
   - Überprüfen Sie im Fenster „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf „Installieren“.
   - Am Ende des Installationsfensters klicken Sie auf „Beenden“.

B.2 Manuelle Oracle-Instanzerstellung (optional)

Zur Vereinfachung empfiehlt Novell, das Sentinel-Installationsprogramm zum Erstellen der Oracle-Instanz während der Installation der Sentinel-Komponenten zu verwenden. Diese Prozedur wird jedoch in dem Fall bereitgestellt, wenn der DBA aus Unternehmensgründen die Oracle-Instanz erstellen muss. Die Tabellenbereiche müssen genau wie angegeben benannt werden.

In der Oracle-Instanz müssen Sie folgende Elemente konfigurieren:

- Parameter
- Tabellenbereiche

So erstellen Sie eine Oracle-Instanz:

1. Melden Sie sich als Oracle-Benutzer an.
2. Verwenden Sie den Oracle-Datenbankassistenten und erstellen Sie Folgendes:

   Hinweis: Die Werte können je nach Systemkonfiguration und Anforderungen variieren. Wenden Sie sich an den DBA.

Tabelle B-1 *Empfohlene Mindestwerte für die Solaris-/Linux-Konfigurationsparameter*

Empfohlene Mindestwerte für die Solaris-/Linux-Konfigurationsparameter	
Parameter	**Größe (in Byte, wenn nicht anders angegeben)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tabelle B-2 *Empfohlene Mindestgröße für den Solaris-/Linux-Tabellenbereich*

Empfohlene Mindestgröße für den Solaris-/Linux-Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
REDO	3x100M	Mindestwert. Erhöhen Sie diesen Wert, wenn die Ereignisrate hoch ist.
SYSTEM	500 M	Mindestwert (autoextend aktiviert)
TEMP	1 G	Mindestwert (autoextend aktiviert)
UNDO	1 G	Mindestwert (autoextend aktiviert)
ESENTD	5 G	Mindestwert
		Für Ereignisdaten (autoextend aktiviert)
ESENTD2	500 M	Mindestwert
		Daten für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
ESENTWFD	250 M	Für iTrac-Daten (autoextend aktiviert)
ESENTWFX	250 M	Für iTrac-Index (autoextend aktiviert)
ESENTX	3 G	Mindestwert
		Für den Ereignisindex (autoextend aktiviert)

Empfohlene Mindestgröße für den Solaris-/Linux-Tabellenbereich

Tabellenbereich	Beispielgröße	Hinweise
ESENTX2	500 M	Mindestwert
		Index für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
SENT_ADVISORD	15 G	Mindestwert, wenn Advisor erworben wird.
		Für Advisor-Daten (autoextend aktiviert).
SENT_ADVISORX	15 G	Mindestwert, wenn Advisor erworben wird.
		Für Advisor-Index (autoextend aktiviert)
SENT_AUDITD	250 M	Mindestwert
		Für Sentinel-Überwachungsdaten (autoextend aktiviert)
SENT_AUDITX	250 M	Mindestwert
		Für Sentinel-Überwachungsindex (autoextend aktiviert)
SENT_LOBS	100 M	Mindestwert in Basisinstallation
		Für große Datenbankobjekte (autoextend aktiviert)
	2 G	Mindestwert in Installation, wenn die Integration mit dem System der Identitätsverwaltung aktiviert ist.
		Für große Datenbankobjekte (autoextend aktiviert)
SENT_SMRYD	3 G	Mindestwert
		Bei der Aggregation für Zusammenfassungsdaten (autoextend aktiviert)
SENT_SMRYX	2 G	Mindestwert
		Bei der Aggregation für Zusammenfassungsindex (autoextend aktiviert)
SYSAUX	100 M	Mindestwert
		Für Oracle 10g-Überwachung (nicht Sentinel-spezifisch)
		Nur für Oracle 10g erforderlich

3. Führen Sie das Skript `createEsecdba.sh` aus dem Verzeichnis „sentinel\dbsetup\bin“ auf der Sentinel-Installations-CD aus. Dieses Skript erstellt den Benutzer „esecdba“, der für das Hinzufügen von Datenbankobjekten mit dem Sentinel-Installationsprogramm erforderlich ist.
4. Sichern Sie die Datenbank.

Weitere Informationen zur Datenbankinstallation in eine vorhandenen Datenbank erhalten Sie im Abschnitt Kapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31.

Sentinel mit Oracle Real Application Clusters

C

Sentinel 6 ist zum Ausführen einer Oracle-Datenbank mit Real Application Clusters (RAC) zertifiziert. Die unterstützte Oracle-Datenbankversion ist Oracle 10g, Version 2 (64 Bit) mit Real Application Clusters (RAC).

Zusätzlich zu den Standardinstallationsprozeduren für Sentinel gibt es ein paar zusätzliche Schritte zum Installieren und Konfigurieren von Sentinel, wenn Oracle RAC verwendet werden soll:

- Konfigurieren einer Oracle RAC-Datenbank
- Installieren des Sentinel-Datenbankschemas auf Oracle RAC
- Konfigurieren von Dateien mit Verbindungseigenschaften für DAS-Komponenten
- Konfigurieren der Verbindung für Sentinel Data Manager
- Konfigurieren der Verbindung für Crystal Enterprise Server

Diese Schritte werden in diesem Dokument beschrieben.

Hinweis: Stellen Sie vor der Installation der Sentinel 6.0-Software sicher, dass Ihr Oracle-Cluster vorhanden und mithilfe der Oracle RAC-Tools ausgeführt wird.

C.1 Konfigurieren der Oracle RAC-Datenbank

So konfigurieren Sie die Oracle RAC-Datenbank:

- Erstellen Sie die RAC-Datenbank mithilfe des Oracle Database Configuration Assistant-Dienstprogramms.
- Erstellen Sie die erforderlichen Sentinel-Tabellenbereiche, die Sentinel-Daten enthalten.
- Erstellen Sie den Sentinel-Schemaeigentümer „ESECDBA“.
- Installieren Sie die Sentinel-Datenbank.
- Installieren Sie die restlichen Sentinel-Komponenten.
- Konfigurieren Sie die Datei mit den Verbindungseigenschaften

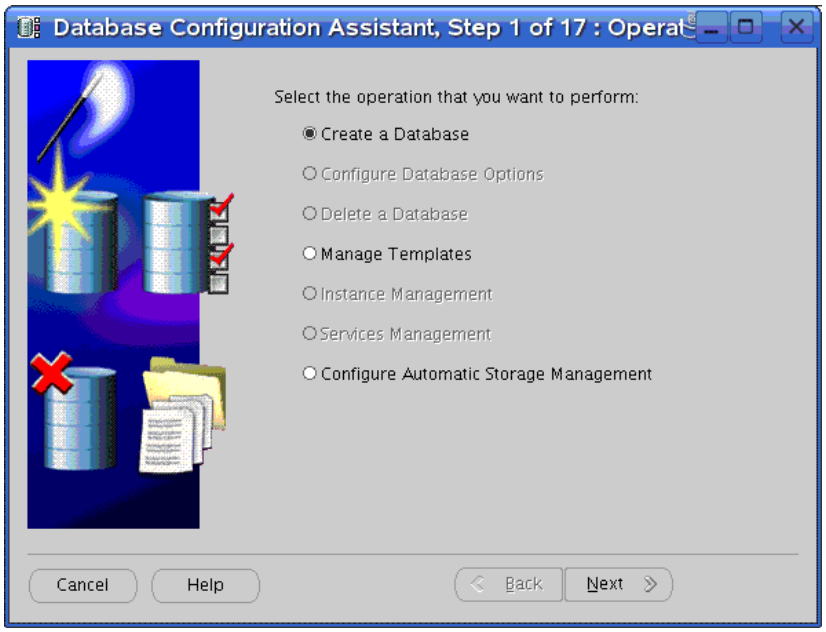
C.1.1 Erstellen der RAC-Datenbank

Mit dieser Prozedur wird eine leere Oracle RAC-Datenbank erstellt, die für die Installation von Sentinel-Komponenten verwendet werden kann. Dieser Prozess verwendet den „Oracle Database Configuration Assistant“ (DBCA).

So erstellen Sie eine RAC-Datenbank:

1. Wählen Sie die „Oracle Real Application Clusters“-Datenbank im DBCA aus. Klicken Sie anschließend auf "Weiter".

2 Wählen Sie aus den Optionen in diesem Bildschirm „Datenbank erstellen“ aus. Klicken Sie anschließend auf "Weiter".

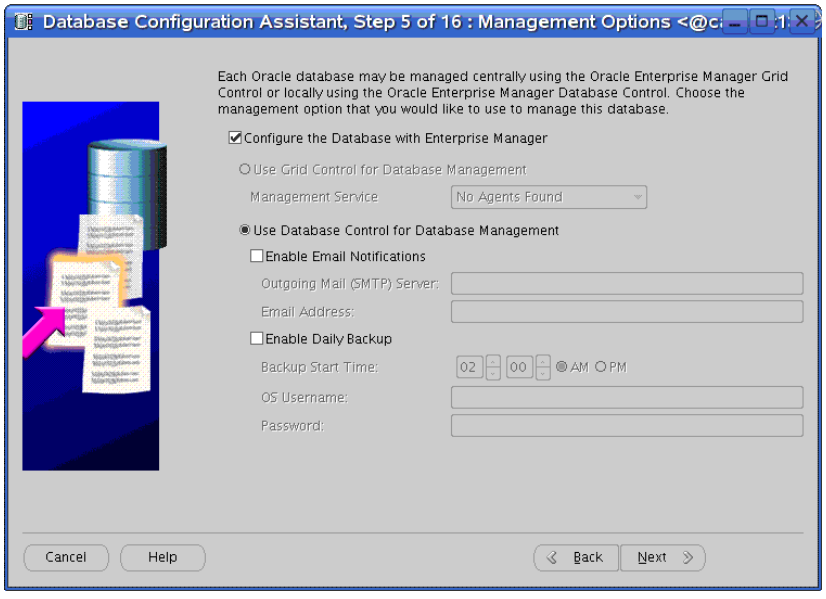


3 Klicken Sie auf „Alle auswählen“, um alle Knoten zum Erstellen der Cluster-Datenbank auszuwählen. Klicken Sie anschließend auf "Weiter".

4 Wählen Sie aus der Liste mit Schablonen eine Schablone aus. Standardmäßig ist der allgemeine Zweck ausgewählt. Klicken Sie anschließend auf "Weiter".

5 Geben Sie den Datenbanknamen und das SID-(Oracle System Identifier-)Präfix an. Klicken Sie anschließend auf "Weiter".

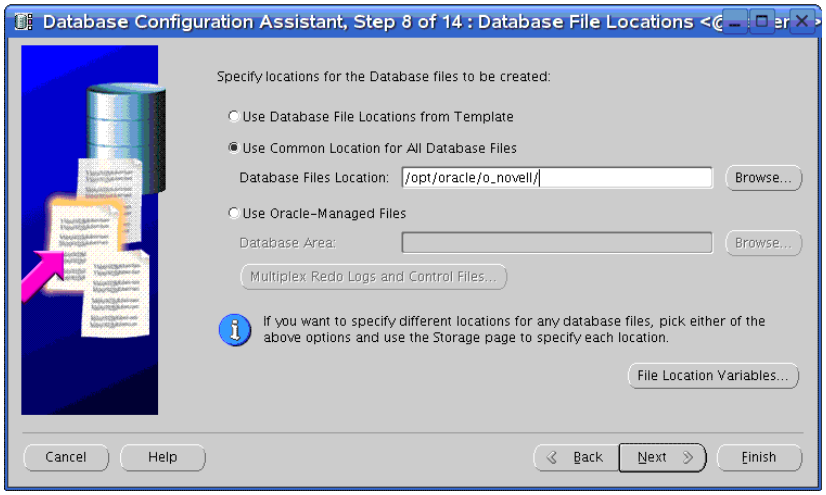
6 Die Standardverwaltungsoption, die zum Verwalten ausgewählt ist, lautet „Configure the Database with Enterprise Manager“ (Datenbank mit Enterprise Manaer konfigurieren). Klicken Sie anschließend auf "Weiter".


Database Configuration Assistant, Step 5 of 16 : Management Options
Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.
Configure the Database with Enterprise Manager
Use Grid Control for Database Management
Management Service
No Agents Found
Use Database Control for Database Management
Enable Email Notifications
Outgoing Mail (SMTP) Server:
Email Address:
Enable Daily Backup
Backup Start Time:
02
00
AM
PM
OS Username:
Password:
Cancel
Help
Back
Next

7 Sie können für alle Benutzerkonten dieselben Passwörter oder verschiedene Passwörter verwenden. Wählen Sie Ihre Option aus und geben Sie die Passwörter an. Klicken Sie anschließend auf "Weiter".

8 Wählen Sie aus den drei Speichermechanismen Cluster-Dateisystem/Automatische Speicherverwaltung/Rohgeräte, die vom System bereitgestellt werden, Ihre Option aus. Wenn Sie „Rohgeräte“ ausgewählt haben, geben Sie den Pfad der Zuordnungsdatei für Rohgeräte an. Klicken Sie anschließend auf "Weiter".

9 Geben Sie ein Verzeichnis an, in dem die Datenbankdateien auf dem Speichersystem platziert werden sollen. Klicken Sie auf Fertig stellen.


Database Configuration Assistant, Step 8 of 14 : Database File Locations
Specify locations for the Database files to be created:
Use Database File Locations from Template
Use Common Location for All Database Files
Database Files Location:
/opt/oracle/o_novell/
Browse...
Use Oracle-Managed Files
Database Area:
Browse...
Multiplex Redo Logs and Control Files...
If you want to specify different locations for any database files, pick either of the above options and use the Storage page to specify each location.
File Location Variables...
Cancel
Help
Back
Next
Finish

10 Behalten Sie die Standardauswahl in den Optionen für die Wiederherstellung und den Fenstern für Beispielschemas bei und klicken Sie auf „Weiter“.

11 Sie können hier einen Datenbankdienst erstellen oder ihn später mit DBCA erstellen.

12 Behalten Sie im Fenster „Datenbankspeicherung“ die Standardauswahl bei. Klicken Sie anschließend auf "Weiter".

13 Wählen Sie aus den Optionen zum Erstellen einer Datenbank „Datenbank erstellen“ aus. Klicken Sie auf Fertig stellen.

C.1.2 Erstellen von Sentinel-Tabellenbereichen

Warnung: Die Sentinel-Installation ist erst dann erfolgreich, wenn alle unten aufgeführten Tabellenbereiche erstellt wurden.

Hinweis: Sie können den Oracle Enterprise Manager oder eine SQL-Abfrage verwenden, um zu überprüfen, ob diese Tabellenbereiche vorhanden sind.

Tabelle C-1 *Empfohlene Mindestgröße für den Tabellenbereich*

Empfohlene Mindestgröße für den Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
Empfohlene Mindestgröße für den Tabellenbereich		
REDO	3 x 100 M	Dies ist ein Mindestwert. Erstellen Sie größere Wiederherstellungsprotokolle, wenn die Ereignisrate hoch ist.
SYSTEM	500 M	Mindestwert (autoextend aktiviert)
TEMP	1 G	Mindestwert (autoextend aktiviert)
UNDO	1 G	Mindestwert (autoextend aktiviert)
ESENTD	5 G	Mindestwert
		Für Ereignisdaten (autoextend aktiviert)
ESENTD2	500 M	Mindestwert
		Daten für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
ESENTWFD	250 M	Für iTRAC-Daten (autoextend aktiviert)
ESENTWFX	250 M	Für iTRAC-Index (autoextend aktiviert)
ESENTX	3 G	Mindestwert
		Für den Ereignisindex (autoextend aktiviert)
ESENTX2	500 M	Mindestwert
		Index für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
SENT_ADVISORD	15 G	Mindestwert, wenn Advisor erworben wird.
		Für Advisor-Daten (autoextend aktiviert)
SENT_ADVISORX	15 G	Mindestwert, wenn Advisor erworben wird.
		Für Advisor-Index (autoextend aktiviert)
SENT_AUDITD	250 M	Mindestwert
		Für Sentinel-Überwachungsdaten (autoextend aktiviert)
SENT_AUDITX	250 M	Mindestwert
		Für Sentinel-Überwachungsindex (autoextend aktiviert)
SENT_LOBS	100 M	Mindestwert in Basisinstallation
		Für große Datenbankobjekte (autoextend aktiviert)
	2 G	Mindestwert in Installation, wenn die Integration mit dem System der Identitätsverwaltung aktiviert ist.
		Für große Datenbankobjekte (autoextend aktiviert)

Empfohlene Mindestgröße für den Tabellenbereich

Tabellenbereich	Beispielgröße	Hinweise
SENT_LOBS	100 M	Mindestwert
		Für große Datenbankobjekte (autoextend aktiviert)
SENT_SMRYD	3 G	Mindestwert
		Bei der Aggregation für Zusammenfassungsdaten (autoextend aktiviert)
SENT_SMRYX	2 G	Mindestwert
		Bei der Aggregation für Zusammenfassungsindex (autoextend aktiviert)
SYSAUX	100 M	Mindestwert
		Für Oracle 10g-Überwachung (nicht Sentinel-spezifisch)

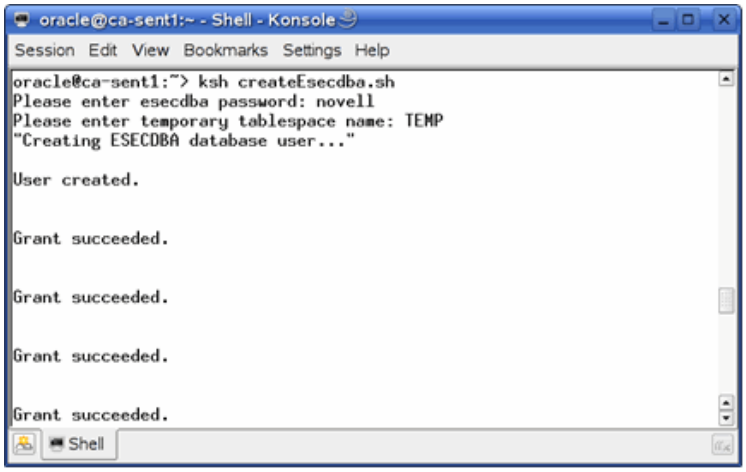
C.1.3 Erstellen von „ESECDBA“

„ESECDBA“ ist der Name des Sentinel-Schemaeigentümers. Für die meisten vom Sentinel-Installationsprogramm erstellten Objekte ist dieser Benutzer der Eigentümer.

So erstellen Sie „ESECDBA“:

1. Suchen Sie das Skript Sentinel-`createEsecdba.sh`auf der Sentinel-Installations-CD unter „disk1/sentinel/dbsetup/bin“.
2. Führen Sie dieses Skript auf einem Computer aus, auf dem der Oracle-Client installiert ist. Möglicherweise müssen Sie das Skript bearbeiten, um die Oracle-Umgebungsvariablen und die „CONNECT AS“-Zeichenfolge korrekt festzulegen (standardmäßig wird das Skript als „sysdba“ verbunden).

   Warnung: Führen Sie dieses Skript nur einmal aus.



C.2 Erstellen der Sentinel-Datenbank

Nachdem die Datenbank konfiguriert ist, müssen Sie die Sentinel-Datenbank erstellen. Diese Prozedur führt die Installation auf einem einzelnen Clusterknoten aus, so als ob es keine RAC-Instanz von Oracle ist.

Sie können das Sentinel-Installationsprogramm auf jedem Computer ausführen, auf dem der Oracle-Client installiert ist, so lange auf dem System die korrekten Oracle-Umgebungsveriablen für den Benutzer „oracle“ festgelegt sind (ORACLE_HOME, ORACLE_BASE). Wenn dieser Computer auch der Sentinel-Server ist, können Sie diese Komponenten gleichzeitig installieren (siehe die Abschnitte oben für Eingabeaufforderungen für Kernkomponenten).

So installieren Sie die Sentinel-Datenbank:

1. Melden Sie sich beim Installationsserver als Stammbenutzer an.
2. Fügen Sie die Sentinel-Installations-CD oder den -Dateisatz ein bzw. mounten Sie sie/ihn.
3. Wechseln Sie zu der CD und doppelklicken Sie auf:

   Für GUI-Modus:

   ```
   ./setup.sh
   ```

   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```
4. Wählen Sie die entsprechende Sprache aus und klicken Sie auf „OK“.
5. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.
6. Lesen und akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf „Weiter“.
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um einen anderen Speicherort für die Installation anzugeben. Klicken Sie anschließend auf "Weiter".
8. Wählen Sie als Installationstyp „Benutzerdefiniert“ (Standard) aus. Klicken Sie anschließend auf "Weiter".
9. Deaktivieren Sie im Fenster „Funktionsauswahl“ nicht benötigte Optionen und wählen Sie „Datenbank“ aus. Klicken Sie anschließend auf "Weiter".
10. Wählen Sie die Ziel-Datenbankserverplattform aus.
    - Wählen Sie aus der Dropdown-Liste „Oracle 10g“ aus.
    - Wählen Sie „Add database objects to an existing database“ (Datenbankobjekte einer vorhandenen Datenbank hinzufügen) aus.

    Klicken Sie anschließend auf "Weiter".
11. Geben Sie die Authentifizierungsinformationen an, um Folgendes zu erstellen:
    - Sentinel-Anwendungsdatenbankbenutzer
    - Sentinel-Administratorbenutzer

    Klicken Sie anschließend auf "Weiter".
12. Es wird eine Zusammenfassung der Datenbankparameter angezeigt. Klicken Sie anschließend auf "Weiter".
13. Die Installationszusammenfassung wird angezeigt. Klicken Sie auf Installieren.

14 Klicken Sie nach der Installation auf „Fertig stellen“.

15 Installieren Sie den Rest des Sentinel-Systems (einschließlich Collector Services, DAS, Communication Server und anderen Sentinel-Komponenten), indem Sie die Informationen in Kapitel 3, „Installieren von Sentinel 6.1“, auf Seite 31 verwenden.

C.3 Konfigurieren der Datei mit den Verbindungseigenschaften

Sie müssen manuell eine Datei mit den Verbindungseigenschaften für die Datenbank mithilfe der Verbindungsinformationen der RAC-Datenbank erstellen. Die Datei mit den Datenbankverbindungseigenschaften sollten auf demselben Computer erstellt werden, auf dem DAS (Data Access Services) installiert ist. Einige der erforderlichen Informationen können in der Datei „$ORACLE_HOME/db/network/admin/tnsnames.ora“ auf den Clusterknoten gefunden werden.

So konfigurieren Sie RAC-Verbindungseigenschaften:

1 Melden Sie sich bei dem Computer an, auf dem die Sentinel Data Access Service (DAS)-Komponenten installiert sind.

2 Ändern Sie das Verzeichnis in „$ESEC_HOME/config“.

3 Erstellen Sie eine Datei mit RAC-Verbindungseigenschaften. Hier ist ein Beispiel, dass für einen Dienst mit Namen OLTP mit drei Knoten erstellt wurde:

```
driver=esecurity.base.db.driver.OracleProxyDriver
dburl=jdbc:esecurity:oracleproxy:@
realdriver=oracle.jdbc.driver.OracleDriver
realdburl=jdbc:oracle:thin:@
fatalvendorstates=28,600,1012,1014,1033,1034,1035,1089,1090,1092,1
094,2396,3106,3111,3113,3114
advancedconnectionstring=(DESCRIPTION=
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent1.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent2.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent3.novell.com) (PORT=1521))
(LOAD_BALANCE=yes)
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=OLTP)
(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=180)
(DELAY=5))))
```

Hinweis: Die gesamte Zeichenfolge „advancedconnectionstring“ muss in einer einzigen Zeile sein.

4 Bearbeiten Sie die Datei `configuration.xml` in „$ESEC_HOME“ und fügen Sie die folgenden Argumente den unten aufgeführten Prozesskomponenten hinzu:

```
-Desecurity.connect.config.file=../config/RACconnect.properties
```

Zu den Prozesskomponenten, die diese Änderung benötigen, zählen:

- DAS_Aggregation
- DAS_Binary
- DAS_iTRAC
- DAS_Query
- DAS_RT

Beispiel:

```
<process component="DAS" depends="UNIX Communication
Server,Windows Communication Server" image=""$(ESEC_JAVA_HOME)/
java" -server -Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml,
/xml/WorkflowMetaData.xml
-Djava.util.logging.config.file=../config/das_query_log.prop
-Djava.security.auth.login.config=../config/auth.login
-Djava.security.krb5.conf=../config/krb5.conf
-Desecurity.execution.config.file=../config/execution.properties -
Dcom.esecurity.configurationfile=../config/configuration.xml
-Desecurity.connect.config.file=../config/RACconnect.properties
-jar ../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" name="DAS_Query" post_startup_delay="20"
type="container" working_directory="$(ESEC_HOME)/data" />
```

5 Starten Sie die Sentinel-Dienste neu, damit die Änderungen an der Datenbankverbindung wirksam werden.

C.4 Konfigurieren der Verbindung für Sentinel Data Manager

Der Wert „advancedconnectionstring“ der Datei „RACconnect.properties“ muss für die Anmeldung bei Sentinel Data Manager verwendet werden.

So melden Sie sich bei Sentinel Data Manager an:

1 Starten Sie den Sentinel Data Manager über „$ESEC_HOME/bin/sdm“.

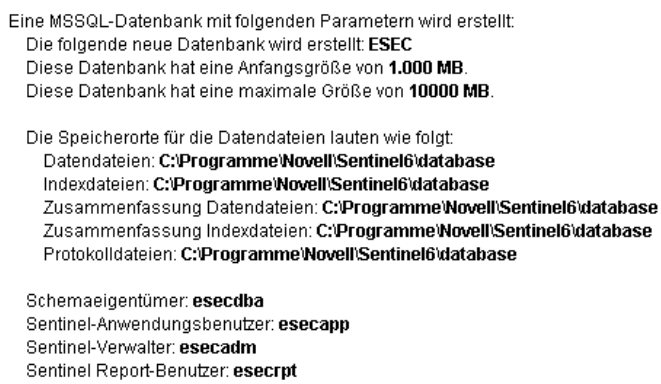
2 Geben Sie Benutzernamen und Passwort für den Sentinel-Datenbankadministrator an (standardmäßig „esecdba“).

3 Kopieren Sie den Wert „advancedconnectionstring“ aus der Datei „RACconnect.properties“.

4 Fügen Sie den Wert „advancedconnectionstring“ in das Feld „Verbindungszeichenkette“ ein.

5 Aktivieren Sie „Verbindungseinstellungen speichern“.

6 Klicken Sie auf "Verbinden".


Eine MSSQL-Datenbank mit folgenden Parametern wird erstellt:
Die folgende neue Datenbank wird erstellt: ESEC
Diese Datenbank hat eine Anfangsgröße von 1.000 MB.
Diese Datenbank hat eine maximale Größe von 10000 MB.
Die Speicherorte für die Datendateien lauten wie folgt:
Datendateien: C:\Programme\Novell\Sentinel6\database
Indexdateien: C:\Programme\Novell\Sentinel6\database
Zusammenfassung Datendateien: C:\Programme\Novell\Sentinel6\database
Zusammenfassung Indexdateien: C:\Programme\Novell\Sentinel6\database
Protokolldateien: C:\Programme\Novell\Sentinel6\database
Schemaeigentümer: esecdba
Sentinel-Anwendungsbenutzer: esecapp
Sentinel-Verwalter: esecadm
Sentinel Report-Benutzer: esecrpt

C.5 Konfigurieren der Verbindung für Crystal

Damit Crystal Enterprise Server die Oracle RAC-Datenbank verwendet, müssen Sie die Datei „tnsnames.ora“ bearbeiten. Die Schritte bei der Standardinstallation für Crystal Enterprise Server müssen befolgt werden, bevor dieser Schritt durchgeführt werden kann.

So bearbeiten Sie die Datei „tnsnames.ora“:

1. Melden Sie sich beim Server mit installiertem Crystal Enterprise Server an und suchen Sie die Datei „tnsnames.ora“.
2. Ändern Sie den Dienst „ESECURITYDB“ so, dass Informationen für alle Knoten angezeigt werden. Die IP-Adresse muss die virtuelle IP-Adresse sein. Eine Beispieldatei für ein System mit drei Knoten wird unten angezeigt:

```
ESECURITYDB =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.1)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.2)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.3)(PORT = 1521))
   (LOAD_BALANCE = yes)
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = REPORT.novell.com)
     (FAILOVER_MODE =
       (TYPE = SELECT)
       (METHOD = BASIC)
       (RETRIES = 180)
       (DELAY = 5)
     )
   )
)
```